DOSSIER ORWELL
Sorveglianza globale

www.guidocontessa.it

La profezia di Orwell avverata e aggravata: tutti spiano tutti

Storia dei sistemi di sorveglianza

PRINT

La tendenza ai sistemi di sorveglianza a circuito chiuso (CCTV) ha origine nel Regno Unito nel 1985: infatti, dopo un anno particolarmente brutto per il calcio inglese e complice l'influsso e l'immagine negativa apportata dai famigerati hooligans, il Football Trust (associazione fondata dalle squadre di calcio inglese) autorizzò l'installazione di sistemi di controllo a circuito chiuso in 92 club. Il passo successivo fu fatto dalla Polizia britannica, la quale installò sistemi di CCTV mobile lungo tutta l'Inghilterra.
Nella totale assenza di regolamentazioni o linee guida, la polizia trovò molteplici utilizzi per questo sistema. La voce si sparse in fretta e il boom dei sistemi CCTV era fatto: ottimo appoggio quando si trattava di presentare l'evidenza delle prove ai processi, il sistema era perfetto anche come "tecnica di controllo sociale".
Telecamere iniziarono a spuntare nel centro di Londra così come nelle piazze principali di varie città, e i cittadini inglesi accolsero con piacere questi strumenti, meritevoli di dare una maggior sicurezza alle donne che tornavano dal lavoro alla sera, o ai bambini nei giardini.
Scuole, ospedali, biblioteche, piazze, vie, negozi.... Ovunque una telecamera ad osservare la folla, le strade, le automobili e le relative targhe degli automezzi.
Sebbene i sistemi CCTV siano utilizzati in altri paesi, nessuno di questi ha avuto un'evoluzione come il Regno Unito: l'evoluzione tecnologica è stata tale che si è arrivati ad un punto per il quale in molti centri urbani questa rete può essere considerata onnipresente. Si è arrivati a considerarli parte integrante del controllo e della lotta alla criminalità: non dimentichiamoci che, quando il mondo intero rimase shockato per le immagini dell'assassinio di un bambino da parte di due suoi amici di 10 anni, l'ultima immagine di James Bulger portato via dal centro città verso i binari abbandonati dove fu poi ritrovato proveniva dai sistemi CCTV del centro di sorveglianza dello shopping center di Liverpool. Le immagini stesse furono usate come prova durante il processo.

Le reti CCTV oggi

Oggi l'industria della sorveglianza visiva britannica spende tra i 150 ed i 300 milioni di sterline all'anno , con un parco di telecamere tra i 200.000 ed i 400.000 pezzi. L'Home Office britannico stima che circa il 95% delle città e dei paesi inglesi si stiano dirigendo verso i sistemi di controllo CCTV per la sorveglianza di aree pubbliche, parcheggi e zone residenziali. La crescita di questo mercato è quantificata dal 15 al 20% all'anno.
Le telecamere stesse sono cambiate - e di molto - dal 1985 ad oggi. Anche in questo caso, come per le reti del patto Ukusa, la tecnologia è progredita, permettendo telecamere antivandalismo, di ridottissime misure, con capacità di "motion detection" e con potenti zoom e dispositivi ad infrarossi, consentendo così anche la visione notturna.
La progettazione degli stessi sistemi è cambiata ed ha sposato tecniche militari di protezione: le nuove installazioni vengono effettuate in modo tale che ogni telecamera controlli sempre la postazione adiacente, fornendo così un controllo incrociato antivandalico ed evitando problemi di sabotaggio, i quali sono sempre esistiti ma raramente sono denunciati, specialmente in Irlanda del Nord. Il governo conservatore di John Major promosse tenacemente l'introduzione di questi sistemi, ed il governo Blair ha continuato per la stessa strada.
Qual è il risultato, oggi ? La più grande rete centralizzata di controllo sulla folla, sui luoghi di comune interesse, sugli avvenimenti di maggior rilievo; un piano su scala nazionale, per il quale entro 5 anni l'Inghilterra completerà la costruzione del più grande sistema di sorveglianza e controllo del traffico stradale il quale, quando sarà terminato, identificherà e seguirà le tracce ed i movimenti di praticamente tutti i veicoli della nazione.
Socialmente, questa tecnologia ha influenzato - e non di poco - le abitudini degli inglesi: nella città di Brighton, ad esempio, la polizia concede la licenza per i superalcoolici o per un locale pubblico solamente se lo stesso è dotato di sistema CCTV interfacciato con la polizia locale.
Abbiamo quindi una tecnologia che fornisce la soluzioni a problemi quali vandalismo, uso di droghe, alcolismo, molestie sessuali o razziali, creazione di disordine pubblico...I sistemi sono stati anche utilizzati per monitorare dimostranti durante manifestazioni.
I problemi nascono però, come nel caso di Echelon, dall'interfacciamento di questi dati con i database... Quello che il governo inglese non dice è che tutte le telecamere inglesi sono state interfacciate a due strumenti estremamente potenti: il Plate Tracking System e il Facial Recognition System.

Le nuove tecnologie

Il Plate Tracking System (P.T.S.) permette alle telecamere, mediante l'interfacciamento con data base esterni, di riconoscere le targhe delle autovetture, e ricercare quindi gli automezzi indicati dal sistema centrale.
Nel Regno Unito per esempio il sistema multifunzionale di gestione del traffico (Traffic Master) utilizza il riconoscimento delle targhe per mappare e gestire gli ingorghi autostradali. Tecnologie P.T.S. sono state installate anche in Svizzera, lungo la A1 Autobahn tra Zurigo e Berna.
Il Facial Recognition System (F.R.S.) permette invece di individuare e riconoscere tra la folla dei visi, delle facce le cui immagini sono immagazzinate negli archivi centrali di più Intelligence o corpi di polizia, nazionali ed internazionali. La tecnologia più utilizzata è il Mandrake System, il quale in teoria può riconoscere le caratteristiche facciali di un viso nel momento stesso in cui appaiono sullo schermo .
Il pericolo nasce quindi dall'interfacciamento di queste reti e questi sistemi con gli archivi esterni. La Video Surveillance sta diventando una infrastruttura nazionale e, forse, il governo USA utilizza già queste strutture per scopi di propria sicurezza nazionale.
Pensiamo però se - come nel caso di Echelon - queste tecnologie venissero utilizzate per scopi commerciali: immaginiamo le targhe delle automobili dei dirigenti di importanti compagnie e multinazionali, continuamente seguite e rilevate; immaginiamo personaggi politici o di rilievo nazionale ed internazionale, costantemente monitorizzati nei loro spostamenti.
Spero che molti dei lettori abbiano visto la scorsa stagione cinematografica il film "Nemico Pubblico", con Gene Hackman e Will Smith: nella storia la NSA era in grado di monitorare attraverso i satelliti, con scarti di pochi metri e una definizione di immagine molto vicina alla perfezione, gli spostamenti di persone e cose. Questo mediante una serie di filtri e controlli incrociati su telefonate, onde radio, dati sensibili (movimenti bancari, archivio telefonate, chiamate a pager, celle di provenienza chiamata, etc..) immagini via satellite e tracking via P.T.S. e F.R.S. Allo stato attuale e nel momento in cui scrivo, la tecnologia in possesso della NSA e del patto Ukusa, unita agli "archivi" on-line del patto EU-FBI, fanno di questo magnifico film - del quale consiglio caldamente la visione - un insieme di informazioni e tecnologie arretrate e "not updated"....nonostante il film sembri fantascienza pura !
Nell'agosto di quest'anno gli Usa hanno lanciato "Ikonos-1", il più potente "image-satellite" commerciale mai realizzato. Le sue lenti paraboliche sono capaci di riconoscere oggetti di piccolissime dimensioni ovunque sulla faccia della Terra. Il satellite, di proprietà della Space Imaging di Denver, Colorado, è il primo di una nuova generazione di satelliti spia ad alta risoluzione di immagine, i quali utilizzano tecnologia ufficialmente riservata alle agenzie di sicurezza governativa. Altre dieci compagnie hanno ottenuto le licenze per effettuare lanci di satelliti simili, e quattro di esse hanno pianificato di effettuare i lanci entro la fine del 1999.
Mercoledì 12 agosto, invece, un missile Titan 4 dell'aeronautica militare statunitense è esploso mentre si innalzava in cielo dalle rampe della base di Cape Canaveral, in Florida. La base del missile era destinata a mettere in orbita un satellite Vortex, commissionato alla Lockeed dal National Reconnaissance Office, un'agenzia governativa di Intelligence. E i Vortex, come illustrato nella sezione Echelon di questo articolo, costituiscono la vera e propria ossatura satellitare del sistema di intercettazioni Echelon. Il satellite era destinato a coprire aree di importanza strategica per il governo Usa, quali Pakistan e India, Cina e Medio Oriente; il costo del satellite si aggira sul miliardo di dollari...
L'impatto che i sistemi CCTV e le tecnologie correlate hanno creato nei confronti dei diritti, delle libertà, della privacy e della vita pubblica del singolo individuo è dunque molto, molto profondo. La distanza, la differenza tra la salvaguardia del cittadino e il calpestare i diritti privati di un essere umano è molto piccola. Hanno esagerato con Echelon, chi ci dice che non faranno lo stesso errore con le reti a CCTV?

23 CCTV: Closed Circuit Tele Vision; televisione a circuito chiuso
24 tra i 225 ed i 450 milioni di dollari
25 A seguito dei cortei "June 18" nel centro di Londra durante il 1999, l'High Court inglese ha capovolto la richiesta della polizia di ottenere le fotografie scattate dai giornalisti durante le dimostrazioni, considerando le immagini dei sistemi CCTV pubblici e privati adeguate per le esigenze della polizia e quindi utilizzabili legalmente e pienamente
26 In questo caso però la percentuale d'errore può raggiungere il 20%
27 Simon Davies, "Hi-res spy satellite set for launch", Daily Telegraph "connected", 8 luglio 1999

Cellulari e sorveglianza

La prossima generazione di telefoni cellulari renderà molto più facile per la polizia esercitare una sorveglianza nascosta sui cittadini, affermano gli attivisti britannici per le libertà civili.

Essi mettono in guardia che la combinazione di tecnologia che rivela la posizione, inserita nei telefoni, e i diritti concessi alla polizia tramite la Legge britannica sulla Regolamentazione dei Poteri Investigativi (RIP) significa che i possessori di tali telefoni potranno e saranno controllati.
Ora gli attivisti stanno avvisando la gente che utilizzare uno dei nuovi telefoni potrebbe rendere estremamente duro mantenere la propria privacy.
Riconoscendo tali implicazioni, le compagnie telefoniche stanno cercando un sistema per consentire ai clienti di nascondere dove si trovano premendo un bottone. Quantunque i cellulari GSM esistenti possono essere utilizzati come congegni di localizzazione, possono soltanto dare una posizione entro cento o duecento metri. Questa accuratezza può essere migliorata se i cellulari sono muniti di uno speciale software che può dare una posizione nel raggio di 50 metri da quella effettiva. Le più nuove tecnologie di telefonia mobile come la General Packet Radio Services (GPRS) e Universal Mobile Telecommunication Services (UMTS) hanno inseriti dei sistemi di localizzazione anche più precisi. Si prevede che i servizi GPRS saranno ampiamente disponibili verso la fine dell'anno, mentre le reti telefoniche UMTS dovrebbero entrare in funzione nel 2002.
Ma Caspar Bowden, direttore della Fondazione per la Ricerca sulla Politica dell'Informazione, avverte che la LEgge sulla Regolamentazione dei Poteri Investigativi appena approvata potrebbe far sì che i dati vengano usati per uno scopo più sinistro. Egli afferma che la Legge RIP considera le informazioni usate per localizzare i telefoni come "dati sulle comunicazioni" e che la polizia non ha bisogno di un mandato per ottenerli. Quindi la polizia potrebbe usare questa informazione per effettuare su chiunque una sorveglianza nascosta usando tali telefoni.

WIKIPEDIA

Divulgazioni sulla sorveglianza di massa del 2013

Da Wikipedia, l'enciclopedia libera.

> **Questa voce o sezione sull'argomento storia è ritenuta da controllare**.
> **Motivo**: *traduzione troppo letterale di una pagina di en.wiki che pecca di recentismo e disorganizzazione meglio ridistribuire i contenuti fra PRISM, Tempora, NSA e Snowden*

Con **divulgazioni sulla sorveglianza di massa del 2013** si fa riferimento ad una serie di inchieste giornalistiche pubblicate dal mese di giugno del 2013 e volte a rivelare dettagli sulle operazioni di sorveglianza e compromissione di massa, messe in atto dall'Agenzia per la Sicurezza Nazionale statunitense (NSA) in complicità con servizi di intelligence di altri paesi, sia nei confronti di cittadini e istituzioni statunitensi che stranieri.

Tali inchieste sono iniziate alla fine del 2012, quando Edward Snowden ha iniziato a mettere a disposizione di alcuni giornalisti numerosi documenti top secret collezionati durante la sua attività per l'NSA. I primi documenti riservati sono stati pubblicati il 6 giugno 2013 dai quotidiani *The Washington Post* e *The Guardian*, attirando una notevole attenzione da parte del pubblico e del resto dei media[1].

Le prime attività di sorveglianza di massa negli Stati Uniti sono iniziate negli anni 1940, per poi essere notevolmente estese nel corso degli anni 1970, assumendo portata globale grazie al programma ECHELON[2]. Nel 2013, grazie alle rivelazioni di Snowden, sono stati svelati nuovi programmi di sorveglianza di massa, quali PRISM, XKeyscore e Tempora[3]. Tali programmi di spionaggio sono attuati in collaborazione con varie agenzie straniere, in particolare quelle dei paesi dell'accordo UKUSA, un'alleanza tra Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti volta a raccogliere informazioni attraverso attività di SIGINT, e vedono come obiettivi privati cittadini e istituzioni di vari paesi, inclusi alleati occidentali degli Stati Uniti e membri della NATO[4]. Come confermato dal direttore dell'NSA Keith B. Alexander il 26 settembre 2013, ad esempio, l'NSA raccoglie e custodisce sistematicamente informazioni sui tabulati telefonici di tutti i cittadini statunitensi[5]; nonostante il presidente Obama e lo stesso Alexander durante i mesi precedenti avessero più volte negato l'esistenza di un qualsiasi tipo di spionaggio domestico[6]. L'enorme quantità di dati raccolti sono conservati in impianti di stoccaggio di grandi dimensioni, come lo Utah Data Center, una struttura di oltre un milione di metri quadri dal costo stimato di 1,5 miliardi di dollari[7].

Come risultato di tali divulgazioni, diversi movimenti, tra cui Restore the Fourth, sono nati per protestare contro le attività di sorveglianza; l'Electronic Frontier Foundation si è unita ad una coalizione di vari gruppi per avviare azioni legali contro l'NSA; mentre l'amministrazione statunitense si è vista costretta a gestire tensioni diplomatiche con paesi alleati e non[8]. Snowden, con il sostegno di varie associazioni per la tutela dei diritti umani, quali Amnesty International, Human Rights Watch, Transparency International e Index on Censorship[9][10][11][12], il 14 giugno 2013 è stato incriminato in accordo con l'Espionage Act del 1917 con l'accusa di furto di proprietà governativa. In seguito gli è stato concesso un temporaneo asilo politico in Russia, il che ha contribuito a deteriorare le relazioni diplomatiche tra il governo russo e statunitense[13][14].

Indice

Cenni storici

Prime attività di intercettazione statunitense

Durante la seconda guerra mondiale, il Regno Unito e gli Stati Uniti attuarono una serie di accordi per la condivisione delle intercettazioni delle comunicazioni dei nemici[15]. Nel marzo 1946, per mantenere in vita tali accordi anche a guerra conclusa, fu siglato un nuovo patto segreto, il British-US Communication Intelligence Agreement, noto come BRUSA[16]. Nel 1945 fu messo in piedi l'ormai defunto Project SHAMROCK, creato per intercettare tutte le comunicazioni telegrafiche da e verso gli Stati Uniti[17][18]. Più tardi le maggiori compagnie telefoniche statunitensi, tra le quali Western Union e ITT World Communications, aiutarono il governo degli Stati Uniti in un primo tentativo di accedere alle reti di comunicazione globale[19].

Mentre alcune agenzie si dedicavano alle comunicazioni internazionali, l'FBI, sotto la guida di John Edgar Hoover, portava avanti una vasta attività di intercettazione nei confronti di molti personaggi pubblici, tra cui Albert Einstein[20], Frank Sinatra[21], Eleanor Roosevelt[22], Marilyn Monroe[23], John Lennon[24] e Martin Luther King Jr.[25], indicato in un memo dell'FBI come «il più pericoloso e potente leader negro negli USA»[26]. Molte di tale attività vennero esposte al pubblico già durante lo scandalo Watergate[27].

L'NSA nacque segretamente nel 1952, per volontà del presidente Harry Truman[28].

Sorveglianza di massa a livello globale: il programma ECHELON

(EN)

«Imagine a global spying network that can eavesdrop on every single phone call, fax or e-mail, anywhere on the planet. It sounds like science fiction, but it's true. Two of the chief protagonists - Britain and America - officially deny its existence. But the BBC has confirmation from the Australian Government that such a network really does exist.»

(IT)

«Immaginate una rete di spionaggio globale in grado di intercettare ogni singola telefonata, fax o e-mail, ovunque sul pianeta. Sembra fantascienza, ma è vero. Due dei protagonisti - Gran Bretagna e USA - negano ufficialmente la sua esistenza. Ma la BBC ha ricevuto conferma da parte del governo australiano che una rete del genere esiste davvero.»

(Articolo della BBC del 3 novembre 1999[29])

Nel 1988, un articolo intitolato *Somebody's listening*[30], scritto da Duncan Campbell sul *New Statesman*, riportò per la prima volta l'esistenza del programma ECHELON[31]. Avviato da Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti, insieme noti come AUSCANNZUKUS, e basato sull'accordo UKUSA, era nato con lo scopo di monitorare le comunicazioni

militari e diplomatiche dell'Unione Sovietica durante la guerra fredda[32]. Anche se la sua esistenza era già nota, l'UKUSA agreement divenne ufficialmente pubblico solo nel 2010.

Con il passare degli anni, divenne una rete di intercettazione globale. Negli anni 1990, il sistema ECHELON era in grado di intercettare comunicazioni satellitari, telefonate tradizionali, traffico internet e trasmissioni a microonde. Il suo funzionamento venne descritto nel 1996 nel libro *Secret Power*, di Nicky Hager. Nonostante l'esistenza di ECHELON continuò ad essere ufficialmente negata da vari esponenti del governo statunitense, fu invece confermata da un'indagine del Parlamento europeo del 2001[2], la quale lo definì un «sistema globale di intercettazione di comunicazioni private e commerciali»[32][33].

Effetti dell'11 settembre e fughe di notizie precedenti Snowden

Dopo gli attentati dell'11 settembre 2001, la portata delle attività di intercettazione negli Stati Uniti aumentò esponenzialmente. Allo scopo di evitare il ripetersi di tali eventi, fu siglato il Patriot Act, cui seguirono altri provvedimenti della stessa natura. Tra questi anche il Protect America Act, che rimuove la necessità di un mandato per l'esecuzione di intercettazione nei confronti di obiettivi stranieri[34], e il FISA Amendments Act.

Tra il 2005 e il 2012, *Wired* svelò l'esistenza del sistema di raccolta dati STELLARWIND, voluto dal presidente Bush poco tempo dopo gli attacchi dell'11 settembre[35]. Il programma, il quale prevede l'analisi di metadati raccolti monitorando il traffico internet, oltre che da altri tipi di telecomunicazione, venne continuato dall'amministrazione Obama. Nel marzo del 2012, in particolare, la rivista pubblicò un articolo che faceva riferimento alla costruzione negli Stati Uniti di un centro di sorveglianza di massa di vaste proporzioni[36], il quale divenne presto oggetto di un'interrogazione parlamentare. In tale interrogazione, il direttore dell'NSA Keith B. Alexander negò la veridicità di quanto dichiarato da *Wired*, negando anche l'esistenza di un qualsiasi tipo di programma di sorveglianza di massa sui cittadini statunitensi[37].

Le rivelazioni sulla sorveglianza di massa del 2013

Tra fine 2012 e i primi mesi del 2013, Edward Snowden consegnò tra i 15 e i 20 mila documenti top secret ai giornalisti del *The Guardian* Glenn Greenwald e Laura Poitras[38]. Dal 6 giugno 2013, il quotidiano inglese iniziò a pubblicare parte di tali documenti, portando alla luce come l'NSA abbia messo in piedi una complessa rete di spionaggio, basata su programmi come PRISM, XKeyscore e Tempora, in grado di intercettare il traffico internet e telefonico di utenti di ogni parte del mondo. A tal fine l'NSA ha usufruito oltre al supporto di altre istituzioni statunitensi, quali l'FBI o il Dipartimento di Giustizia, anche di importanti società private, tra le quali Verizon, Telstra, Google e Facebook.

Fondamentale è stata anche la collaborazione dei servizi di intelligence straniera, per accedere ai principali punti di snodo delle telecomunicazioni sparsi per il mondo. Oltre ai servizi degli altri paesi, soprannominati i "cinque occhi", che hanno siglato l'accordo UKUSA, ossia il Defence Signals Directorate australiano, il Communications Security Establishment canadese, il Government Communications Security Bureau neozelandese e il Government Communications Headquarters britannico, l'NSA ha cooperato con agenzie di varia nazionalità, tra cui il Bundesnachrichtendienst tedesco, l'Unit 8200 israeliano e il National Defence Radio Establishment svedese, il quale ha dato accesso ai cavi sotto al mar baltico[39].

Scopi e obiettivi della sorveglianza di massa

Nati con la giustificazione della lotta al terrorismo e la preservazione della sicurezza nazionale, i vari programmi di sorveglianza sono stati estesi a pieno campo ed impiegati impropriamente ed illecitamente per valutare la politica estera e la stabilità economica di altri paesi, e per raccogliere informazioni riservate di natura commerciale industriale, anche riguardanti soggetti privati; ciò anche allo scopo di avvantaggiare l'amministrazione statunitense durante le trattative durante la preparazione di trattati internazionali o accordi di natura economica con altri paesi[40][41].

Segue un elenco di alcuni obiettivi della rete di sorveglianza dell'NSA svelati tra i mesi di giugno e ottobre 2013[42].

- L'NSA colleziona metadati sulle telefonate effettuate attraverso tutti i gestori statunitensi.
- Una speciale divisione dell'agenzia chiamata "Follow the Money" raccoglie dati sulle transazioni finanziarie di soggetti privati da importanti istituti internazionali come Visa, Mastercard e SWIFT.
- Grazie ad alcuni programmi come Fairview e centri d'ascolto sparsi per il mondo, l'NSA e la CIA sono in grado di accedere ai dati generati dal traffico telefonico e internet anche di altri paesi; i soli paesi "immuni" sono quelli dell'accordo UKUSA, ossia Australia, Canada, Nuova Zelanda e Regno Unito. Il 31 luglio 2013 il *The Guardian* riportò l'esistenza del programma XKeyscore, il quale si avvale di una rete di 500 server segreti i quali registrano «quasi tutto quello che fa un utente medio su internet»[43].
- Attraverso il programma di sorveglianza PRISM l'NSA ha accesso diretto ai server di molte delle principali aziende dell'informatica statunitense, quali Microsoft, Google, Yahoo!, Facebook, Apple, YouTube e Skype. Alcune di tali aziende hanno anche collaborato con l'NSA per craccare i sistemi di criptaggio dei dati utilizzati. L'agenzia monitora quindi le attività degli utenti, compresi scambi di messaggi, foto e video, conservando in particolare le liste di indirizzi utente usate nei servizi e-mail e di messaggistica istantanea. Secondo un articolo del *Washington Post* in un solo giorno del 2012 l'agenzia ha collezionato oltre 400.000 indirizzi mail solo da Yahoo![44].
- Sono stati spiati anche capi di stato o di governo, tra cui Dilma Rousseff (Brasile), Felipe Calderón (Messico) e Angela Merkel (Germania). In particolare, l'agenzia avrebbe intercettato i telefoni personali di 35 leader politici stranieri, tra cui il cellulare privato di Angela Merkel[45]. Tra gli organi di governo stranieri spiati, figurano il Ministero dell'Energia brasiliano e il Ministero per gli affari esteri francese, oltre che vari componenti del governo indiano.
- In collaborazione con la CIA, l'NSA ha piazzato strumenti di intercettazione in circa 80 tra ambasciate e consolati in tutto il mondo[46].
- Sono state spiate anche diverse sedi della NATO, dell'ONU, dell'Unione europea, e loro funzionari di primo livello, tra cui il segretario generale Ban Ki-moon[46][47][48]. Attività di spionaggio sono state condotte anche in occasione di summit internazionali, in cui sono finiti nel mirino degli agenti segreti vari diplomatici e leader politici.
- Tra le attività di spionaggio industriale, sono finite nel mirino dell'NSA anche Google, Petrobras, società leader nella trivellazione nelle profondità marine[49], e SWIFT.
- Nel 2006 l'NSA inserì una backdoor in uno dei principali standard di codifica addirittura del National Institute of Standards and Technology, istituto guida americano responsabile di definire le norme di sicurezza del cyberspazio.

Nomi dei programmi e sistemi utilizzati

Tra i principali programmi di sorveglianza e software svelati dai documenti di Snowden sono presenti:

- PRISM, programma per il monitoraggio del traffico generato da vari fornitori di servizi elettronici e telematici, compresi Apple, Microsoft, Facebook, Google e Skype.
- Boundless Informant, programma per la gestione dei dati raccolti.
- Tempora, programma di sorveglianza elettronica e telematica del British Government Communications Headquarters.
- XKeyscore, programma per l'analisi del traffico internet generato da utenti al di fuori degli Stati Uniti.
- Mail Isolation Control and Tracking, sistema di tracciamento della posta ordinaria, con il collezionamento di tutti gli indirizzi usati.
- Fairview, programma per l'intercettazione delle telecomunicazioni originate al di fuori degli Stati Uniti.
- Dropmire, programma per le intercettazioni all'interno di ambasciate e consolati stranieri.
- Genie, nome in codice di una botnet utilizzata per infiltrarsi in reti protette.
- Bullrun, nome derivante dall'omonima battaglia, è un software per l'analisi del traffico internet criptato.
- Edgehill, nome derivante dall'omonima battaglia, è l'equivalente di Bullrun utilizzato da British Government Communications Headquarters.

WIKIPEDIA

ECHELON

Da Wikipedia, l'enciclopedia libera.

Echelon (parola di origine francese, in italiano *scaglione*) è una denominazione utilizzata dai media e nella cultura popolare per descrivere la raccolta di *signal intelligence* (SIGINT) e analisi dei segnali gestita per conto dei cinque stati firmatari dell'accordo UKUSA di sicurezza (Australia, Canada, Nuova Zelanda, Regno Unito e gli Stati Uniti, noto come AUSCANNZUKUS o *cinque occhi*).[1][2] È stato anche descritto come l'unico sistema software che controlla il download e la diffusione della intercettazione di comunicazioni via satellite.[3]

Per estensione, la *Rete Echelon* indica il sistema mondiale d'intercettazione delle comunicazioni private e pubbliche.

Il sistema venne per la prima volta portato all'attenzione pubblica dal direttore dell'Omega Foundation, Steve Wright, quando firmò nel 2000 il rapporto della STOA (Scientific and Technologies Options Panel of the European Parliament) sull'argomento, dal titolo *Prison technologies: An Appraisal of the Technologies of Political Control*:[4][5]da quel momento indagini del Parlamento europeo, e non solo, approfondiranno ed estenderanno la ricerca sull'argomento.

Un impianto di Echelon a Menwith Hill (Gran Bretagna)

Indice

Origine del nome

La commissione temporanea del Parlamento europeo descrive il sistema Echelon con queste parole:[6]

(EN)	(IT)

> «It seems likely, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that its name is in fact ECHELON, although this is a relatively minor detail.»
>
> («Sembra probabile, viste le prove e le numerose dichiarazioni di molte persone e organizzazioni, tra cui anche le fonti degli Stati Uniti, che il suo nome sia, effettivamente, ECHELON, anche se questo è un dettaglio relativamente meno importante.»
>
> (*On the existence of a global system for the interception of private and commercial communications*)

L'ex dipendente della NSA Margaret Newsham ha sostenuto di aver lavorato alla configurazione e all'installazione di software che costituisce il sistema ECHELON mentre lavorava alla Lockheed Martin, dal 1974 al 1984 a Sunnyvale in California e a Menwith Hill in Inghilterra.[7] In quel periodo, secondo Newsham, il nome in codice Echelon era anche il nome della rete dei computer della NSA. Lockheed lo chiamò *P415*. I software del programma erano chiamati *Silkworth* e *SIRE*. Un satellite chiamato *Vortex* serviva per intercettare le informazioni. Un'immagine, disponibile su internet, estrapolata da un lavoro di descrizione, mostra "Echelon" elencato insieme a molti altri nomi in codice.[8]

Creazione della struttura

L'infrastruttura satellitare è stata insediata all'inizio degli anni sessanta (nel periodo della guerra fredda) con la messa in orbita di un gran numero di satelliti spia, ognuno dei quali prese il nome di una differente generazione tecnologica corrispondente a una cosiddetta *costellazione*: ne sono alcuni esempi *Ferret*, *Canyon*, *Rhyolite* e *Aquacade Ocelot*.

Misawa Air Base (MSOC)

Responsabile di questi progetti è stata la *National Security Agency* (NSA), la principale agenzia di spionaggio statunitense che agiva in collaborazione con la CIA e il supersegreto *National Reconnaissance Office* (NRO).

Dopo il tramonto della guerra fredda, negli anni novanta sono stati approntati dei sistemi tecnologicamente più evoluti, ovvero i satelliti spia di classe *Trumpet*, *Lacrosse*, *KH11*, *Mercury* e *Mentor*.

I centri elaborazione dati terrestri si trovano a *Menwith Hill* (Gran Bretagna), a *Pine Gap* (Australia) e presso la *Misawa Air Base* (Honshū, Giappone). Il controllo esecutivo degli insediamenti è gestito dagli Stati Uniti. A questi siti va aggiunta l'Isola di Ascensione (isola situata nell'Oceano Atlantico), che rappresenta (o rappresentava) una base strategica non citata tra i siti ufficiali del progetto Echelon.[9]

Funzionamento

Echelon utilizza le intercettazioni dei cavi sottomarini del genere Aquacade e Magnum per controllare tramite i suoi più importanti centri di invio le trasmissioni di Internet, in particolare lo smistamento di messaggi e-mail.

Data l'enorme mole di dati sorvegliata, impossibile da analizzare da parte di esseri umani, per intercettare i messaggi "sospetti" (inviati via e-mail, telefono, fax ecc.) viene utilizzato un sistema basato sull'identificazione di parole chiave e loro varianti, in grado anche di rintracciare l'impronta vocale di un individuo.

Non si sa molto su come funzioni il meccanismo e di quali coperture goda: quello che è certo è che nel 1997, in seguito al processo di due ragazze pacifiste, in alcuni documenti e testimonianze, la British Telecom ha fatto sapere che tre linee a fibre ottiche (con la capacità di centomila chiamate simultanee ciascuna), passavano per il nodo di *Menwith Hill*. La vicenda ha fatto

capire che non si può amministrare una società di telecomunicazioni senza far parte del tavolo di Echelon. Gli accordi telefonici Echelon sono blindati, obbligano le compagnie telefoniche occidentali ad assegnare la sicurezza delle aziende a uomini del controspionaggio. In Italia, per esempio, Marco Bernardini, testimone chiave dell'inchiesta sui dossier illegali raccolti dalla Security Pirelli-Telecom, effettuò intercettazioni per conto di Echelon sull'Autorità Antitrust ed ebbe accesso ai dati di Vodafone e Wind.[10]

Su Echelon sono state sollevate, negli anni, numerose interpellanze al Parlamento europeo, il quale ha aperto nel 2001 una commissione temporanea sul caso.[5] Sempre il Parlamento europeo, alla vigilia degli attentati alle torri gemelle, deliberò una serie di contromisure per contrastare Echelon.[11]

In passato si è sospettato che il sistema possa essere stato utilizzato anche per scopi illeciti, come lo spionaggio industriale, a favore delle nazioni che lo controllano, a discapito delle aziende di altri Paesi, anche se a loro volta aderenti alla NATO.

Capacità operative

Il sistema era in grado di intercettare diversi tipi di comunicazioni, a seconda del mezzo utilizzato (ad esempio via radio, via satellite, via microonde, via onde radio o fibra ottica).[6] Durante la seconda guerra mondiale e fino agli anni '50 le onde radio ad alta frequenza (HF) venivano spesso utilizzate per comunicazioni militari e diplomatiche,[12] e potevano essere intercettate a grandi distanze.[6] La crescita di comunicazioni satellitari attraverso l'utilizzo di satelliti geostazionari degli anni '60 diede un'ulteriore possibilità di intercettare le comunicazioni. Sempre il Parlamento europeo nel 2001 dichiarò:

> «Se gli stati aderenti all'UKUSA operano stazioni di ascolto in regioni di rilievo della terra, in via di principio possono intercettare tutte le telefonate, i fax e il traffico dati trasmessi attraverso questi satelliti»
>
> ([6])

Echelon in Italia

In Italia la notizia dell'esistenza della rete di monitoraggio globale Echelon è stata oggetto di un'inchiesta del giornalista Claudio Gatti pubblicata sul nr.12 del settimanale economico IL MONDO del 20 marzo 1998. Quarantadue giorni dopo, il Capo del Governo Romano Prodi ha risposto in Parlamento ad una interrogazione dell'onorevole Domenico Carratelli del Partito Popolare Italiano sostenendo che il Governo italiano non era a conoscenza dell'esistenza di tale sistema di intercettazione (Camera dei Deputati seduta nr. 346 del 24 aprile 1998).

Non è stato mai confermato un coinvolgimento in Echelon della base USA di Gioia del Colle, nota per le vicende legate alla cosiddetta strage di Ustica.

Recentemente si è accertato il coinvolgimento della base USAF, in collaborazione con la CIA, a San Vito dei Normanni presso Brindisi, non più operativa dal 1994.[13][14] Nella zona era visibile fino alla fine degli anni novanta la struttura dell'antenna Wullenweber installata, un'antenna di tipo AN/FLR-9, in gergo "gabbia degli elefanti", del tutto simile a quella presente presso la base navale di Rota, in Spagna[15]. La base di San Vito era diventata operativa durante la prima metà degli anni sessanta, con un raggio utile di intercettazione delle comunicazioni radio di 2.400 km. Dieci anni dopo la chiusura della base brindisina, nel 2004, è stata chiusa la base tedesca di Bad Aibling.[16]

Panorama dell'impianto di Echelon a Menwith Hill nel 2005.

Cultura di massa

- Sulle vicende riguardanti Echelon nel 2006 è stato realizzato il film *The Listening - In ascolto*;
- Nel film *The Bourne Ultimatum - Il ritorno dello sciacallo* (2007), la CIA riesce tramite Echelon ad intercettare una fuga di notizie su un progetto segreto denominato "Blackbriar";
- Nella trama del videogioco cyberpunk *Deus Ex*, ambientato nel 2052, si allude ad un certo *Echelon IV*, programma avente le stesse funzioni del suo antenato ma migliorato e spostato nell'Area 51;
- Nella trama della serie di videogiochi *Splinter Cell* vi sono riferimenti ad Echelon, fra cui il più importante è il nome dell'agenzia di spionaggio per la quale il protagonista Sam Fisher lavora: *Third Echelon*.

Note

1. **^** Google books - Echelon (http://books.google.com/books?id=1x6Akzkxv5IC&printsec=frontcover&source=gbs_summary_r&cad=0) by John O'Neill
2. **^** *AUSCANNZUKUS Information Portal*, auscannzukus.net.. URL consultato il 1º febbraio 2010 (archiviato dall'url originale il 29 dicembre 2010).
3. **^** (**EN**) James Bamford, *Body of Secrets*. Anchor, 2002. ISBN 0-385-49908-6
4. **^** *An Appraisal of the Technologies of Political Control* (**PDF**), su *europarl.europa.eu*.
5. *Relazione sull'esistenza di un sistema d'intercettazione globale per le comunicazioni private ed economiche (sistema d'intercettazione Echelon) (2001/2098 (INI))* (http://www.privacy.it/ueEchelon.html) del Parlamento europeo, 11 luglio 2001
6. Gerhard Schmid, *On the existence of a global system for the interception of private and commercial communications (Echelon interception system), (2001/2098(INI))* (**PDF**), European Parliament: Temporary Committee on the Echelon Interception System, 11 luglio 2001. URL consultato il 27 marzo 2008.
7. **^** (**EN**) Bo Elkjær, Kenan Seeberg, *Echelon WAS MY BABY*, in *Cryptome*, Ekstra Bladet, 17 novembre 1999. URL consultato l'8 maggio 2011 (archiviato dall'url originale il 15 giugno 2006).*"Unfortunately, I can't tell you all my duties. I am still bound by professional secrecy, and I would hate to go to prison or get involved in any trouble, if you know what I mean. In general, I can tell you that I was responsible for compiling the various systems and programs, configuring the whole thing and making it operational on mainframes"*; *"Margaret Newsham worked for the NSA through her employment at Ford and Lockheed from 1974 to 1984. In 1977 and 1978 Newsham was stationed at the largest listening post in the world at Menwith Hill, England...**Ekstra Bladet** has Margaret Newsham's stationing orders from the US Department of Defense. She possessed the high security classification TOP SECRET CRYPTO."*
8. **^** *Names of Echelon associated projects – image without any context* (**JPG**), su *ladlass.com*. URL consultato l'8 maggio 2011 (archiviato dall'url originale il 27 febbraio 2008). All'interno di *Interception Capabilities 2000 - PART 1*, su *ladlass.com*. URL consultato l'8 maggio 2011 (archiviato dall'url originale il 5 gennaio 2008).
9. **^** Filler AG. *Echelon, l'isola che ascoltava il mondo (Wired Magazine) (http://www.wired.it/magazine/archivio/2009/01/storie/Echelon,-l%27isola-che-ascoltava-il-mondo.aspx?page=2) Archiviato (https://web.archive.org/web/20090606153421/http://www.wired.it/magazine/archivio/2009/01/storie/echelon,-l%27isola-che-ascoltava-il-mondo.aspx?page=2) il 6 giugno 2009 in Internet Archive.*
10. **^** Ruggiero Capone, «I misteri atlantici di Telecom ed Echelon», *Liberal*, 6 gennaio 2010.
11. **^** Punto Informatico, 7 settembre 2001
12. **^** *The Codebreakers*, Ch. 10, 11
13. **^** San Vito dei Normanni in GoogleMaps (https://maps.google.it/maps?ie=UTF8&hl=it&ll=40.647466,17.840209&spn=0.014066,0.043945&t=h&z=15)
14. **^** *Echelon, individuata l'antenna italiana*, su *mediamente.rai.it*. URL consultato il 5 maggio 2011 (archiviato dall'url originale il 28 luglio 2011).
15. **^** Base navale di Rota in GoogleMaps (https://maps.google.it/maps?f=q&hl=it&geocode=&q=36%C2%B0+39%E2%80%B2+23.63%E2%80%B3+N,+6%C2%B0+21%E2%80%B2+53.84%E2%80%B3+W&ie=UTF8&ll=36.656439,-6.364968&spn=0.012635,0.027466&t=h&z=16&iwloc=addr)
16. **^** Base tedesca di Bad Aibling in GoogleMaps (https://maps.google.it/maps?f=q&hl=it&geocode=&q=47%C2%B052%E2%80%B2N+12%C2%B001%E2%80%B2E&ie=UTF8&ll=47.880319,11.984432&spn=0.006217,0.021973&t=h&z=16).

Bibliografia

- Duncan Campbell. *Il mondo sotto sorveglianza. Echelon e lo spionaggio elettronico globale*, Eleuthera, 2003 (traduzione di Guido Lagomarsino), ISBN 88-85060-72-2
- Patrick Radden Keefe. *Intercettare il mondo: Echelon e il controllo globale*, Einaudi, 2006 (traduzione di Piero Arlorio), ISBN 88-06-18179-3

Voci correlate

- Asse del Male
- Pine Gap
- SIGINT
- SORM
- Carnivore (software)
- San Vito Air Station
- Wullenweber
- Progetto per un nuovo secolo americano
- PRISM (programma di sorveglianza)

Altri progetti

- Wikimedia Commons (https://commons.wikimedia.org/wiki/?uselang=it) contiene immagini o altri file su **Echelon (https://commons.wikimedia.org/wiki/Category:Echelon?uselang=it)**

Collegamenti esterni

- ControSpionaggio Satellitare: Il sistema di intercettazione Echelon (http://www.osdife.org/intelligence.html) Dott. Gavino Raoul Piras su OSDIFE Università di Roma Tor Vergata.
- Echelon (https://web.archive.org/web/20150227175058/http://www.globalsecurity.org/intell/systems/echelon.htm) su GlobalSecurity (http://www.globalsecurity.org/index.html)
- *Raul Chiesa parla dell'Echelon*, su *apogeonline.com*. URL consultato il 15 maggio 2013 (archiviato dall'url originale il 26 novembre 2012).
- Echelon (http://www.fas.org/irp/program/process/Echelon.htm) su F.A.S. (https://web.archive.org/web/20100328133210/http://www.fas.org/index.html)
- *Interrogazione parlamentare al caso San Vito Air Station*, su *italy.peacelink.org*.
- Vi racconto tutti i segreti di Echelon, articolo de la Repubblica
- Il Caso Echelon, Università degli studi di Pisa
- La UE Vota: Echelon esiste e va bloccato (http://punto-informatico.it/77626/PI/News/ue-vota-Echelon-esiste-va-bloccato.aspx) articolo di Punto Informatico.

Carnivore (software)

Da Wikipedia, l'enciclopedia libera.

Carnivore (conosciuto anche come **DCS1000** che significa Digital Collection System) è il nome dato ad un sistema, analogo ad un network tap, implementato dall'FBI (Federal Bureau of Investigation), nei suoi laboratori di Quantico (Virginia). Grazie all'utilizzo di questa tecnologia le e-mail vengono controllate così come le conversazioni telefoniche. È una forma di controllo di polizia.

Indice

Storia

Questo sistema è stato messo in funzione dai servizi segreti americani nel periodo immediatamente successivo all'attacco al World Trade Center l'11 settembre 2001 per controllare il traffico in rete e prevenire ulteriori attacchi terroristici.

Con questa piattaforma è possibile intercettare il traffico sui protocolli di navigazione HTTP, FTP, SMTP, e POP3, inviato o diretto a tutte le porte.

L'esistenza di Carnivore viene resa nota il 4 luglio 2000, quando il quotidiano statunitense Wall Street Journal scrive per la prima volta dell'esistenza di Carnivore, nello stesso periodo in cui il senato americano stava dibattendo sul suo possibile impiego.

Soltanto il 26 ottobre 2002 il governo USA concede il via libera per l'utilizzo su larga scala come conseguenza dell'attacco all'America. DCS1000 da allora viene, infatti, inserito all'interno del pacchetto di misure anti-terrorismo chiamato *Patriot Act*[1] per contrastare il terrorismo mondiale ed in particolare l'organizzazione di Al-Qaeda.

Il progetto Carnivore è derivato da una precedente esperienza molto simile denominata "Omnivore", che già permetteva di focalizzare l'attenzione su un particolare utente, controllarlo in ogni suo movimento nel cyberspazio oltre a consentire un'analisi approfondita su tutta la posta elettronica, e dal sistema di sorveglianza "Echelon", messo in atto dalla National Security Agency (NSA) durante il periodo della Guerra Fredda.

Si tratta, quindi, di un programma in grado di filtrare i pacchetti di dati che transitano tra l'utente e il provider e di ricostruire i messaggi scambiati: posta elettronica, pagine web visitate e conversazioni in diretta (chat).

Carnovire può essere definito come uno sniffer, con la differenza che i normali sniffer permettono a chiunque l'accesso come amministratore per controllare il flusso di dati il tipo di indagini che si stanno svolgendo; questo sistema, invece, analizza il traffico della rete solo dopo averlo copiato: in questo modo nessuno può conoscere la quantità e il tipo di informazioni intercettate.

Il Pacchetto Carnivore

- Sistema operativo Windows NT (o Windows 2000);
- 128 MB di RAM Processore Pentium III, disco rigido da 4-18 GB di spazio in disco e un drive lomega Jaz da 2 Gb sul quale vengono salvati i dati;
- La macchina non ha uscite TCP/IP per evitare intrusioni da parte degli Hacker;
- Sistema hardware di autenticazione per controllare gli accessi alla macchina impedendo accessi non autorizzati;
- Software scritto in C++ (si distinguono tre diversi programmi: Carnivore, Packeteer, Coolminer).

Il sistema

Il sistema si compone di un computer collegato presso un provider, che copia tutti i dati: esso si inserisce nel segmento della rete in cui si trova la persona sospetta, non interagisce, né intralcia il flusso comunicativo, limitandosi esclusivamente a copiarlo.

I pacchetti di dati così copiati con il software Carnivore vengono automaticamente analizzati da un filtro che cerca le parole o i termini considerati motivo di sospetto dalla polizia federale americana; tutto il materiale ininfluente viene, al contrario, eliminato, anche per occupare il minor spazio possibile in memoria.

I dati vengono trasmessi tramite linea telefonica al client "Packeteer" che ricostruisce i file sulla base delle intercettazioni, il risultato viene successivamente inviato agli operatori federali con l'aiuto del terzo software del pacchetto chiamato "Coolminer", salvato e copiato su un particolare tipo di disco Jaz che quotidianamente viene scaricato dagli uomini dell'FBI.

Le operazioni di copiatura dei dati non rallentano il flusso comunicativo, per cui la presenza di Carnivore nel server è impercettibile; non si tratta di un sistema molto veloce, ma in grado comunque di elaborare milioni di e-mail al secondo.

Il costo del pacchetto è stimato intorno ad un milione di euro.

La procedura per l'installazione del DCS1000 è molto semplice: una volta individuato il soggetto sospetto da controllare, l'FBI chiede al giudice l'autorizzazione per le intercettazioni, specificando che le informazioni rientrano nell'ambito di un'inchiesta penale.

Ottenuto il permesso viene ricercato il provider interessato e si installa il pacchetto che è molto simile alla scatola nera degli aerei, perfettamente sigillata. Periodicamente i poliziotti scaricano e verificano i dati raccolti.

Il governo statunitense potrà confermare o negare il funzionamento del sistema, ma ci sono alcuni aspetti che generalmente sono accettati. Un computer per essere accessibile deve essere fisicamente installato in un ISP o in un'altra locazione dove si può "sniffare" il traffico per cercare messaggi email in transito. La tecnologia non richiede niente di particolare, basta usare un comune packet sniffer o qualcosa di simile (come uno script perl ad esempio).

Si può ottenere la cooperazione degli ISP o dei gestori di una LAN dove installare Carnivore sia volontariamente sia su mandato; una volta che il sistema è piazzato non è solo abilitato a catturare semplicemente ogni email che attraversa il sistema, ma può anche inviare un avvertimento nominando specifiche persone o email che possono essere monitorate. Quando una email equivale a questi criteri, il messaggio viene annotato con le informazioni desiderate come la data, l'ora, il destinatario e il mittente. Tale intercettazione può anche essere inviato immediatamente all'FBI, ma attualmente non si conoscono i dettagli.

Dal momento in cui è stata resa nota l'esistenza di questo sistema, sono nate controverse polemiche legate alle possibili violazione della privacy che questo nuovo strumento di sorveglianza poteva facilmente attaccare: i difensori della sfera privata hanno iniziato una mobilitazione per frenare la curiosità di Carnivore

In particolare tra le misure preventive per tutelare la libertà personale rientra la creazione di programmi anti-Carnivore come il software criptografico chiamato "Antivore" lanciato dalla software House ChainMail; oppure "Camera Sky" in grado di nascondere i dati eludendoli al controllo del DCS1000, infine altri due software come "Freedom" ideato da "Zeroknowledge" e quello della società "NetworIce".

L'FBI ha sempre sostenuto che il DCS100 non avrebbe pregiudicato la privacy dei navigatori poiché, grazie a filtri speciali (che possono essere modificati all'insaputa del provider), esso è in grado di intercettare solo le informazioni sensibili, una rassicurazione non priva di polemiche.

Inoltre, il già citato, "Patriot Act" fornisce alla polizia informatica americana la libertà di perseguire Hacker stranieri accusati di avere commesso crimini sulla rete degli USA.

La polizia federale ha ammesso di avere usato Carnivore in venticinque casi di cui sedici nel 2000 d cui sei criminali e dieci di spionaggio e terrorismo.

Ci sono diverse speculazioni riguardo l'implementazione, l'uso, e i possibili abusi di Carnivore. Ma i fautori di Free speech e dei diritti civili sono interessati sul potenziale di questo strumento.

L'assistente del direttore dell'FBI Director Donald Kerr ha affermato:

> *Il sistema Carnivore funziona più o meno come uno "sniffer" e altri strumenti di diagnostica delle reti usati dagli ISP quotidianamente, tranne che fornisce all'FBI l'unica abilità di distinguere tra comunicazioni che potrebbero essere o non essere legittimamente intercettate. Per esempio, se un mandato prevede l'intercettazione legale di un tipo di comunicazione (per esempio, e-mail), ma esclude gli altri (per esempio, online shopping) lo strumento può essere configurato a intercettare solo e-mail che vengono trasmesse da e per un certo nome. È un analizzatore di reti molto specializzato che funziona come un applicativo su un normale PC sotto il sistema operativo Microsoft Windows. Funziona come "sniffing" di una determinata porzione di rete e copiando e memorizzando solo i pacchetti che uguagliano precisamente un definito filtro configurato in conformità al mandato. Questo filtro può essere molto complesso e fornisce all'FBI la capacità di raggruppare trasmissioni che si conformano ai mandati scritti, ai mandati "trap & trace", agli ordini di intercettazione Titolo III, ecc. È importante distinguere ora cosa significa "sniffing." Il problema di discernere tra i messaggi degli utenti di Internet è complesso. Tuttavia ciò che esattamente Carnivore fa è che non cerca nel contenuto di ogni messaggio collezionando quelli che contengono una certa parola come "bomba" o "droga", ma seleziona i messaggi basati su criteri espressi nel mandato, per esempio, messaggi trasmessi da e per un particolare account o utente. cryptome.org (http://cryptome.org/carnivore-rf.htm)*

L'FBI non si è però fermata a Carnivore iniziando ad utilizzare nuovi sistemi tra i quali: Dragon Ware utile per tracciare ogni movimento del sospetto in rete e "Magic Lantern". Quest'ultimo funzione come un "Trojan Horse" (letteralmente "Cavallo di Troia"), un programma che si installa sul computer del soggetto da controllare e compie una serie di attività tra le quali quella di registrare i tasti premuti sulla tastiera in modo da captare parole sospette (come attentati, terrorismo, ecc.) oltre a fornire chiavi di accesso, password e modalità di decifrazione dei documenti criptati. Il meccanismo che permette di rilevare la chiave di accesso in gergo è chiamato "Keylogging", cioè memorizza le parole inserite dalla tastiera in un file particolare che, una volta elaborato, permette di risalire alla parola chiave. In questo modo, potendo vedere i tasti è possibile risalire a password, testi scritti, programmi eseguiti, indirizzi internet visitati.

La polizia federale americana non ha mai voluto rendere pubblico il codice sorgente di questo sistema per tre ragioni:

- Perché gli hacker potrebbero violare il sistema;
- Perché esso è protetto da copyright e quindi non è possibile diffonderlo per esigenze contrattuali;
- La legislazione degli Stati Uniti (Titolo 18 Sezione 2512 del Codice) impedisce la diffusione di apparecchiature studiate per spiare clandestinamente le comunicazioni di altre persone.

Nonostante questo, la legge americana sulla libertà di informazione ha consentito all'EPIC (Electronic Privacy Information Center) di ottenere 565 pagine di documenti riservati su Carnivore, alcune delle quali sono però state in parte mascherate con inchiostro indelebile tra cui proprio quelle del codice sorgente.

Dopo i prolungati attacchi della stampa, l'FBI ha cambiato il nome di questo sistema da "Carnivore" a "DCS1000."

A metà gennaio 2005 l'FBI essenzialmente abbandona Carnivore in favore di software commerciali[2]. Le motivazioni che hanno spinto la polizia federale verso questa scelta riguardano le forti critiche dell'opinione pubblica contro questo sistema più volte accusato di violare la libertà personale dei cittadini.

Altre applicazioni pratiche

> **Questa voce o sezione sull'argomento internet non cita le fonti necessarie o quelle presenti sono insufficienti**.

Esiste, infine, un'altra faccia di Carnivore. Un gruppo di net-artisti interessati alla sperimentazione digitale i "Radical Software Group" (RSG) di New York, hanno clonato il software creato dalla polizia federale americana, per utilizzarlo con degli scopi diversi. Si tratta di una piattaforma situata nella loro città per la net-art chiamata "CarnivorePE", che ha lo scopo di catturare i pacchetti di dati e trasformarli successivamente in musica, immagini o filmati; in questo modo i dati diventano arte.

Il programma è stato messo a disposizione dal RSG di una vasta comunità di altri artisti. Tra questi, un gruppo di italiani chiamato "Limiteazero" ha visto in Carnivore una nuova forma di ready made. Essi hanno sperimentato due forme di arte con questo sniffer: una sperimentazione software chiamata *"Actiwe Metaphore"* (2002) e una hardware denominata *"Network is Speaking"* (2004).

La prima traduce gli indirizzi e i dati intercettati in forme tridimensionali, movimenti e suoni, in questo modo il flusso dei dati, normalmente percepibile solo dalla macchina, viene reso visibile a tutti. La seconda, invece, è un'installazione molto complessa allestita a Milano, essa ricorda la forma di Idra dove le dodici teste del mostro sono rappresentate da 12 monitor LCD appesi al soffitto.

Infine, altri due esempi di arte emergente riguardano: "Policestate" che converte i dati catturati in movimenti per modellini delle macchinine radio comandate dalla polizia, con movimenti a volte disordinati e altre organizzati in modo da formare vere e proprie coreografie; "Word Wide Painters" che trasforma i dati ricevuti in graffiti sul muro, talvolta riproducendo le bandiere dei paesi di provenienza dei soggetti spiati, i loro indirizzi IP o i siti a cui si connettono, naturalmente in assoluto rispetto della privacy degli utenti.

Note

1. **^** Le mani dell'FBI su Internet | Diritto online | Webnews (http://webnews.html.it/news/leggi/3594/le-mani-dellfbi-su-internet/) Archiviato (https://web.archive.org/web/20060607215552/http://webnews.html.it/news/leggi/3594/le-mani-dellfbi-su-internet/) il 7 giugno 2006 in Internet Archive.
2. **^** *FOXNews.com - FBI Ditches Carnivore Surveillance System - Politics*, su *foxnews.com*. URL consultato il 15 febbraio 2005 (archiviato dall'url originale il 22 agosto 2006).

Voci correlate

- Digital Collection System Network

- Sniffing, intercettazione passiva dei dati nella rete
- Magic Lantern software, lo strumento di login simultanea dell'FBI
- Regulation of Investigatory Powers Act, provvedimento legale inglese per l'intercettazione digitale
- ECHELON, programma di intercettazione digitale mondiale
- DragonWare Suite, programma FBI per immagazzinare le informazioni di siti web
- Total Information Awareness
- Patriot-Act, insieme di misure anti-terrorismo adottate negli USA dopo l'11 settembre 2001

Collegamenti esterni

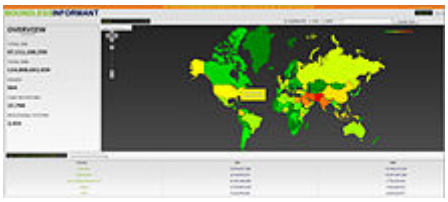
- (EN) *Cryptome on Carnivore*, su *cryptome.org*.
- (EN) *Wired on Carnivore*, su *wired.com*.
- (EN) *EPIC on Carnivore*, su *epic.org*.

PRISM (programma di sorveglianza)

Da Wikipedia, l'enciclopedia libera.

PRISM è un programma di sorveglianza elettronica, cyberwarfare e Signal Intelligence, classificato come di massima segretezza, usato per la gestione di informazioni raccolte attraverso Internet e altri fornitori di servizi elettronici e telematici. È stato posto in attività dalla National Security Agency (NSA) fin dal 2007.[1] PRISM è il nome in codice scelto dal governo statunitense per US-984XN, ispirandosi al prisma ottico ("un mezzo trasparente alla luce che ha la capacità di alterare la visione della realtà osservata attraverso di esso").[2] I documenti pubblicati da Edward Snowden (ex impiegato di una società informatica che lavora per la NSA) nel giugno 2013 descrivono il programma PRISM come abilitato alla sorveglianza in profondità su comunicazioni dal vivo di gran parte del traffico Internet mondiale e delle informazioni memorizzate. I dati ottenibili comprendono quindi email, chat, chat vocali e videochat, video, foto, conversazioni VoIP, trasferimento di file, notifiche d'accesso e dettagli relativi a siti di reti sociali. Per ottenere ciò, PRISM si serve della collaborazione di vari fra i maggiori service provider, tra cui i principali sono Google, Facebook, Microsoft, Skype, Apple, Yahoo, AOL e altri;[3][4] inoltre, esso sfrutta le caratteristiche di routing tipiche della Rete: in particolare, il fatto che il percorso seguito dai pacchetti IP durante le connessioni non sia necessariamente il più breve ma piuttosto quello più economico. Grazie a tali caratteristiche di routing gran parte del traffico mondiale delle comunicazioni fra utenti e server posti in nazioni diverse (ad esempio un utente italiano che si collega a un sito web cinese) passa per gli Stati Uniti o per ISP statunitensi, circostanza che permette a PRISM di immagazzinare ancor più dati.[5] Il 14 giugno, in un'intervista, Snowden ha dichiarato che la NSA, per ampliare l'area coperta dalle intercettazioni, svolge abitualmente attacchi contro le dorsali Internet mirando ai router più importanti, sia di paesi amici (come gli stati europei), sia di provider cinesi.[6] Nello stesso periodo Snowden dichiarò pure che la NSA aveva svolto azioni del genere su reti cinesi in decine di migliaia di attacchi.[7] L'unica contromisura veramente efficace che i cittadini possono usare per difendersi da PRISM è, secondo Snowden, l'uso di sistemi di crittografia forte (come PGP, Tor e mezzi simili).[8]

Logo del programma PRISM


Mappa della raccolta dati dell'NSA

L'operatività del programma si basa sulle previsioni normative contenute nella sezione 702 del *Foreign Intelligence Surveillance Act* (FISA), una legge promulgata nel 1978 ma più volte modificata (ad esempio, dallo USA PATRIOT Act concepito nel 2001) e prorogata (l'ultima volta da Barack Obama nel dicembre 2013), durante gli anni successivi agli attentati dell'11 settembre 2001.

Il 2 agosto 2013 un articolo del Süddeutsche Zeitung rivela che le operazioni di PRISM non si limitano al solo spionaggio. Da alcuni documenti di cui la testata è in possesso risulta che i maggiori ISP europei e no:

1. svolgono veri e propri attacchi informatici a reti private;
2. alterano attivamente il traffico utente allo scopo di sfruttare vulnerabilità (tramite exploit) e installare trojan su determinati computer, compromettono così sistemi informatici onde ottenerne controllo completo al pc delle vittime.

Gli ISP coinvolti vengono definiti "la Crème de la Crème" di Internet, in quanto da soli hanno il controllo quasi totale sul traffico Internet mondiale.[9] [10]

Indice

Risposta delle presunte società coinvolte

Gli articoli del *Washington Post* e del *Guardian* riportano che i dati raccolti da PRISM provenivano direttamente dai server degli Internet Service Provider.[1]

Dirigenti aziendali di diverse società individuate nei documenti trapelati hanno comunicato al *The Guardian* che non erano a conoscenza del programma PRISM e, in particolare, hanno anche negato di rendere disponibili su vasta scala tali informazioni al governo, come riportato dai quotidiani.[11]

Elenco delle società, ordinate per data in cui si sono unite al progetto PRISM

Note

1. (EN) Barton Gellman e Laura Poitras, *US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, in *The Washington Post*, 6 giugno 2013. URL consultato l'11 giugno 2013.
2. ^ (EN) *Prisms - definition of Prisms*, su *Free Online Dictionary*.
   «A medium that misrepresents whatever is seen through it».
3. ^ (EN) *NSA leaks hint Microsoft may have lied about Skype security*, su *Russia Today*.
4. ^ (EN) *NSA leak fallout: LIVE UPDATES*, su *Russia Today*.
5. ^ (EN) *'How little rights you have:' Anonymous leaks more PRISM-related NSA docs*, su *RT.com*.
6. ^ (EN) *Edward Snowden claims US hacks Chinese targets. The US has perpetrated hacking attacks on "hundreds" of targets in Hong Kong and mainland China since 2009, the former CIA analyst Edward Snowden has claimed.*, su *telegraph.co.uk*.
   «We hack network backbones – like huge internet routers, basically – that give us access to the communications of hundreds of thousands of computers without having to hack every single one," Edward Snowden su Telegraph».
7. ^ (EN) *Snowden's asset: NSA hacking exposer knows secrets China wants*, su *RT.com*.
8. ^ (EN) *Edward Snowden's live Q&A: eight things we learned*, in *The Guardian*.
   «Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.».

9. **^** (EN) *Telecom giants give GCHQ unlimited access to networks, develop own spyware – Snowden leaks*, su *RT.com*.
«...Such software could come in a form of Trojan viruses installed on targeted computers, the reports say, stating that the companies' involvement in data collection is much larger and more complicated than previously thought... (...Tale software può apparire sotto forma di virus trojans installati sui computer dell'obiettivo, dice il report, affermando che il coinvolgimento delle aziende nella raccolta dati è molto più vasto e complicato di quanto precedentemente pensato...)».
10. **^** (DE) *Internet-Überwachung: Snowden enthüllt Namen der spähenden Telekomfirmen*, in *Süddeutsche Zeitung*.
«...Bislang geheime Powerpoint-Folien, die der SZ vorliegen, zeigen, was der britische Geheimdienst GCHQ alles kann: Installation von Trojanern, Desinformation, Angriffe auf Netzwerke. .... und welche privaten Internetanbieter beim Ausspähen behilflich sind. Es ist die Crème de la Crème der Branche, mit Macht über große Teile der weltweiten Internetstruktur... (Dalle presentazioni Powerpoint, che il Süddeutsche Zeitung ha ricevuto, emerge che il GCHQ britannico può tutto: Installazione di Virus Trojan, Disinformazione, Attacco alle Reti. ... viene poi rivelato quali ISP privati collaborano allo spionaggio. Sono la "Crème de la Crème" dell'industria, controllano la maggior parte dell'infrastruttura globale di Internet)».
11. **^** (EN) Cyrus Farivar, *New Leak Shows Feds Can Access User Accounts for Google, Facebook and More - Secret Slides Reveal Massive Government Spying, Tech Companies Dispute Reports*, Ars Technica, 6 giugno 2013. URL consultato il 12 giugno 2013.

Voci correlate

- Divulgazioni sulla sorveglianza di massa del 2013
- National Security Agency
- Cyberwarfare
- SORM
- SIGINT
- Spionaggio industriale
- Bullrun
- Echelon
- Sniffing
- Man in the middle
- Replay attack
- Tempora
- Unit 8200

Altri progetti

- Wikimedia Commons (https://commons.wikimedia.org/wiki/?uselang=it) contiene immagini o altri file su **PRISM (https://commons.wikimedia.org/wiki/Category:PRISM_(surveillance_program)?uselang=it)**

Collegamenti esterni

- "The NSA Files (http://www.guardian.co.uk/world/the-nsa-files)." *The Guardian*
- prism-break.org (https://prism-break.org/) Una lista di contromisure per l'autodifesa degli utenti dallo spionaggio di PRISM, scritta dalla FSF

Scoperto un APT mai rilevato in precedenza a livello globale **Leggi...**

Home Page » News

Security News

Mercoledì 11 Gennaio 2017

Eye Pyramid, che cos'è e come scoprire se si è stati infettati

Una complessa attività di indagine denominata ***Eye Pyramid***, condotta dal *Cnaipic, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche* del servizio Polizia Postale e delle Comunicazioni e coordinata dalla Procura della Repubblica di Roma, ha fatto luce su un **esteso sistema di cyberspionaggio** messo in piedi con attacchi informatici di tipo ***APT* (*Advanced Persistent Threat*).**

L'invio di un messaggio di posta elettronica contenente un **allegato malevolo** è alla base della creazione di una **vera e propria centrale di sorveglianza** ai danni di **numerose autorità politiche e militari** di strategica importanza e di **sistemi informatici utilizzati da Stato e altri enti pubblici** come *istruzione.it, gdf.it, bancaditalia.it, camera.it, senato.it, esteri.it, tesoro.it, finanze.it, interno.it.*

A svelare l'esistenza del malware è stata proprio un'email indirizzata ad un amministratore di sistema di un'importante infrastruttura nazionale, al quale non è passata inosservata. L'email, dopo essere stata oggetto di analisi tecnica, è stata segnalata al *Cnaipic, Centro nazionale anticrimine informatico della Polizia Postale.*
Il messaggio di posta elettronica conteneva dunque un tipo di **malware** utilizzato generalmente per le campagne di ***spear phishing***, ovvero phishing focalizzato su uno specifico obiettivo.

I protagonisti del cyberspionaggio si sono avvalsi dunque di una *botnet*, una vasta rete di computer creata infettando i dispositivi con un malware di tipo ***Rat* (Remote access tool)**, che consente, una volta installato, il **pieno controllo da remoto del dispositivo infetto** e che avrebbe permesso dunque agli hacker per lungo tempo di acquisire in maniera silenziosa informazioni riservate per poi riversarle all'interno di server localizzati negli Stati Uniti.

A seguito di queste vicende di cyberspionaggio al centro della cronaca, la cui reale portata è tutt'altro che chiarita, **il nostro team Cert sta operando le necessarie verifiche per**

CONTATTACI

Vedi anche:

- Yarix rilascia il secondo YSOC Security Report
- Sicurezza Convergente 4 Club TI
- Scoperto un APT mai rilevato in precedenza a livello globale
- Offerte di lavoro | Cybersecurity
- Var Group attraverso Yarix acquisisce il 10% di Athesys
- Var Group, Yarix e Darktrace insieme a Cybertech Europe 2019
- WunderVAR | Play your future with Var Group
- Offerta di lavoro | Security Sales Specialist
- Sharing Experiences in Compliance | Bologna 2 ottobre
- Offerta di lavoro | Cybersecurity Manager
- Offerta di lavoro | Junior Security Engineer
- Attacco hacker a Bonfiglioli neutralizzato anche grazie all'intervento di Yarix
- Yarix presenta il primo YSOC Security Report
- Richmond Cyber Resilience Forum, Gubbio 19-21 giugno
- Start Your Industry 4.0
- Vulnerabilità critica in Remote Desktop: Microsoft rilascia le patch anche per Windows XP e Windows Server 2003 (CVE-2019-0708)
- L'exploit ThrAngryCat potrebbe colpire milioni di dispositivi Cisco (CVE-2019-1649 CVE-2019-1862)
- Var Group acquisisce il 60% di Gencom
- YCERT: Analisi di Gootkit, malware all'attacco di PA e aziende

escludere che le reti dei clienti siano state oggetto di violazione mediante utilizzo dello stesso malware.

Per quanti desiderino eseguire dei controlli sui propri PC Windows, mettiamo a disposizione uno script in VBS, di cui si può fare il **download**.

Dalla lettura dell'ordinanza di custodia cautelare predisposta dal GIP si possono infatti estrarre degli elementi utili ad eseguire dei controlli sui sistemi Windows. Il malware utilizzato si appoggia ad un componente commerciale di terze parti (MailBee.NET.dll prodotto dalla Afterlogic co.) per la comunicazione attraverso email.
Questo prodotto è licenziato e la stessa licenza che identifica univocamente il licenziatario è stata utilizzata a partire dalle prime infezioni del malware nel 2010, fino a dicembre 2015.

La chiave di licenza, nelle macchine infette, è registrata in una apposita sezione del registro di sistema. Essendo la chiave parzialmente nota attraverso la lettura dell'ordinanza del GIP (alcune parti non sono correttamente identificabili, a causa della bassa qualità della scansione), è facile verificarne la presenza nel registro. Da analisi già effettuate da altri malware analyst sono emerse altre chiavi di licenze potenzialmente coinvolte.
Per semplificare l'individuazione della chiave di licenza nel proprio PC, abbiamo dunque preparato un semplice **script in VBS**, **che verifica l'eventuale presenza di una delle sottostringhe della chiave di licenza** che, se rinvenute, costituiscono un forte indicatore dell'avvenuta infezione.

Dopo aver aperto il file .zip, al cui interno è presente un file con estensione .vbs, è sufficiente fare un doppio clic sopra.

Gli hash MD5 del file compresso e dello script all'interno sono i seguenti:

053fffd972019704756ee95d9f1e7287 *eyepyramid-check.zip
7c5a986075ade28aaba18d335dd34ef8 *eyepyramid-check.vbs

Reti resilienti a prova di cyber attack... anche in ambienti OT

Var Group ti aspetta al Security Summit Milano

Var Group e Yarix di nuovo in campo con CyberChallenge.IT

Live Webinar Digital Security con Var Group e Microsoft

Offerta di lavoro | Cyber Security Specialist

Var Evolution, l'innovazione vissuta

Blockchain per l'innovazione, Yarix e Var Group investono nella startup Commerc.io.

Sextortion, ricatto in bitcoin con minaccia di divulgazione

Var Group, Yarix e Darktrace insieme a Cybertech Europe 2018

AI e Machine Learning: Kleis entra nella Digital Security Division di Var Group

Offerta di lavoro | Tecnico sistemista

Var Group annuncia la quarta partnership nel segno della sicurezza

La nuova normativa PSD2 tra opportunità e sfide, Milano 28 giugno

Offerte di lavoro | Cyber Security

Richmond Cyber Resilience Forum, Gubbio 21-22 giugno

Security Summit Roma, Seminario Bitdefender - Yarix

Var Group e Yarix Partner di ABI Banche e Sicurezza 2018

BLOCKCHAIN E IMPRESA - 28/03 Camera di Commercio di Firenze

NUOVA PRIVACY - 28/03 Confcommercio di Treviso

Sicurezza Convergente, un approccio olistico

Var Group e la sua Cyber Division Yarix annunciano l'acquisizione del 19% di Blockit

Security Summit Milano, Seminario Bitdefender - Yarix

Offerta di lavoro | IT Security Specialist

Var Group e Yarix Gold Sponsor di ITASEC18

Var Group e Yarix in campo con CyberChallenge.IT

Campagna di malspam minaccia le aziende italiane

Industrial CyberSecurity: Var Group e Yarix a ICS Forum

Breach Compilation: un'imponente risorsa facilita l'accesso a 1,4 miliardi di credenziali

Rischio Cyber e normativa europea GDPR: Milano, 4 dicembre

Grave vulnerabilità in Microsoft Office sfruttata dal gruppo Cobalt

GDPR e Cyber Security nella sanità: Firenze, 30 novembre

GDPR: Var Group e la sua Cyber Division Yarix acquisiscono il 20% di Privatamente

Cyber-raccolta si riferisce all'uso di guerra informatica tecniche per condurre spionaggio . Attività di cyber-raccolta in genere si basano su l'inserimento di minacce informatiche in una rete mirata o un computer al fine di cercare, raccogliere e trapelare informazioni sensibili.

Cyber-collezione iniziata nel lontano 1996, quando la diffusione generalizzata di connettività Internet ai sistemi aziendali del governo e preso slancio. Da quel momento, ci sono stati numerosi casi di tale attività.

Oltre agli esempi di stato sponsorizzato, cyber-raccolta è stato utilizzato anche dalla criminalità organizzata per l'identità e il furto di e-banking e dalle spie aziendali. Operazione High Roller usato agenti cyber-raccolta al fine di raccogliere PC e smart-phone informazioni che è stato utilizzato per razziare elettronicamente conti bancari. Il Rocra , alias Red October, sistema di raccolta è un "di spionaggio per il noleggio" operazione da criminali organizzati che vendono le informazioni raccolte al miglior offerente.

Contenuto

Piattaforme e funzionalità

Strumenti Cyber-raccolta sono stati sviluppati da governi e gli interessi privati per quasi ogni sistema operativo del computer e smart-phone. Gli strumenti sono noti per esistere per Microsoft, Apple e computer Linux e iPhone, Android, Blackberry e Windows Phone. I principali produttori di COTS (COTS) tecnologia di raccolta informatica includono Gamma Group dal Regno Unito e Hacking Team in Italia. Bespoke aziende strumento di cyber-raccolta, molti pacchetti offerta COTS di zero-day exploit, includono Endgame, Inc. e Netragard degli Stati Uniti e VUPEN dalla Francia. Le agenzie di intelligence degli Stati hanno spes[illegible]rie squadre per sviluppare strumenti cyber-raccolta,

- *Scansione di dati* : storage locale e la rete vengono analizzati per trovare e copiare i file di interesse, questi sono spesso documenti, fogli di calcolo, file di progettazione come ad esempio file Autocad e file di sistema come il file passwd.
- *Cattura posizione* : GPS, WiFi, reti e altri sensori allegate sono utilizzati per determinare la posizione e il movimento del dispositivo infiltrato
- *Bug* : il microfono del dispositivo può essere attivato al fine di registrare l'audio. Allo stesso modo, flussi audio destinati altoparlanti locali possono essere intercettate a livello di dispositivo e registrati.
- *Nascosti reti private* che ignorano la sicurezza della rete aziendale. Un calcolo che viene spiato può essere collegato a una rete aziendale legittima che è pesante monitorato per l'attività del malware e allo stesso tempo appartiene a una rete WiFi privata al di fuori della rete aziendale che perde informazioni riservate fuori del computer di un dipendente. Un computer di questo tipo è facilmente impostato da un doppio agente che lavora nel reparto IT per installare una seconda scheda wireless in un computer e un software speciale per monitorare a distanza il computer di un dipendente attraverso questa seconda scheda di interfaccia senza che esse siano a conoscenza di una banda laterale canale di comunicazione tirando informazioni fuori del suo computer.
- *Camera* : le telecamere di dispositivi possono essere attivati in modo da catturare di nascosto immagini o video.
- *Keylogger e mouse Logger* : l'agente di malware in grado di catturare ogni tasto, il movimento del mouse e fare clic che l'utente di destinazione fa. In combinazione con afferra schermo, questo può essere utilizzato per ottenere le password che vengono immessi utilizzando una tastiera virtuale sullo schermo.
- *Schermo Grabber* : l'agente di malware può prendere immagini periodici di cattura dello schermo. Oltre a mostrare le informazioni sensibili che non possono essere memorizzati sulla macchina, come ad esempio i saldi di e-banking e web mail criptata, questi possono essere utilizzati in combinazione con i dati chiave e logger mouse per determinare le credenziali di accesso per altre risorse Internet.
- *Crittografia* : raccolti i dati vengono crittografati di solito al momento della cattura e possono essere trasmessi in diretta o conservati per exfiltration tardi. Analogamente, è pratica comune per ogni specifica operazione utilizzare la crittografia specifica e capacità poli-morfico dell'agente cyber-raccolta al fine di garantire che il rilevamento in una posizione non comprometta altri.
- *Crittografia Bypass* : Poiché l'agente di malware opera sul sistema di destinazione con tutti i diritti di accesso e dell'account utente del bersaglio o amministratore di sistema, la crittografia viene bypassato. Ad esempio, l'intercettazione di audio utilizzando il microfono e dispositivi di uscita audio permette il malware catturare entrambi i lati di una chiamata Skype crittografato.
- *Exfiltration* : agenti Cyber-raccolta di solito trapelare i dati acquisiti in modo discreto, spesso in attesa per il traffico web di alta e mascherare la trasmissione come la navigazione web sicura. Unità flash USB sono stati utilizzati per trapelare informazioni da spazio d'aria dei sistemi protetti. Sistemi exfiltration spesso comportano l'uso di sistemi proxy inversi Anonimizza il ricevitore dei dati.
- *Replicare* : Gli agenti possono replicarsi su altri supporti o sistemi, ad esempio un agente può infettare i file su una condivisione di rete scrivibile o si installare sul drive USB per infettare i computer protetti da un intercapedine d'aria o comunque non sulla stessa rete.
- *Gestione di file e di manutenzione del file* : Il malware può essere usato per cancellare le tracce di sé dai file di log. Si può anche scaricare e installare i moduli o gli aggiornamenti e file di dati. Questa funzione può anche essere utilizzato per piazzare "prove" sul sistema di destinazione, ad esempio, per inserire la pedopornografia sul computer di un politico o di manipolare voti su una macchina elettronica conteggio dei voti.
- *Regole di combinazione* : Alcuni agenti sono molto complesse e sono in grado di combinare le caratteristiche di cui sopra, al fine di fornire capacità di raccolta di informazioni molto mirate. Ad esempio, l'uso di scatole di delimitazione GPS e l'attività del microfono può essere utilizzato per trasformare uno smartphone in un bug intelligente che intercetta le conversazioni solo all'interno dell'ufficio di un bersaglio.
- *Cellulari compromesse* . Dal momento che, cellulari moderni sono sempre più simili a computer di uso generale, questi cellulari sono vulnerabili agli stessi attacchi informatici-collect come sistemi di computer, e sono vulnerabili a trapelare informazioni estremamente sensibili colloquiale e la posizione per un aggressori. Perdite di posizione cellulare GPS e le informazioni colloquiale per un attaccante è stata riportata in una serie di recenti cyber-inseguendo i casi in cui l'attaccante è stato in grado di utilizzare la posizione GPS della vittima a chiamare le imprese e le autorità di polizia nelle vicinanze per fare false accuse contro la vittima a seconda della sua posizione, questo può variare da dire l'informazione personale del ristorante per prendere in giro la vittima, o fare falsa testimonianza contro la vittima. Per esempio se la vittima fosse parcheggiata nel grande parcheggio gli attaccanti possono chiamare e stato che hanno visto droga o l'attività della violenza in corso con la descrizione della vittima e le indicazioni per la loro posizione GPS.

Infiltrazione

Ci sono diversi modi comuni per infettare o accedere al bersaglio:

- Un *proxy di iniezione* è un sistema che è posto a monte del singolo bersaglio o la società, di solito al provider di servizi Internet, che inietta il malware nel sistema target. Ad esempio, una scarica innocenti da parte dell'utente può essere iniettato con l'eseguibile di malware al volo in modo che il sistema di destinazione è quindi accessibile agli agenti del governo.
- *Spear Phishing* : un e-mail con cura artigianale viene inviato al bersaglio al fine di invogliare loro di installare il malware tramite un Trojan documento o di un'unità da un attacco ospitato su un server web compromesso o controllate dal proprietario del malware.
- *Ingresso fraudolento* può essere utilizzato per infettare un sistema. In altre parole, le spie si rompono con molta prudenza in residenza o la sede del bersaglio e installare il malware sul sistema di destinazione.
- Un *monitor di monte* o *sniffer* è un dispositivo in grado di intercettare e visualizzare i dati trasmessi da un sistema di destinazione. Di solito questo dispositivo è posizionato al provider di servizi Internet. Il Carnivore sistema sviluppato dagli Stati Uniti FBI è un famoso esempio di questo tipo di sistema. Sulla base della stessa logica di un'intercettazione telefonica , questo tipo di sistema è di uso limitato oggi a causa dell'uso diffuso di cifratura durante la trasmissione dei dati.
- Un *infiltrazione wireless* sistema può essere utilizzato in prossimità del bersaglio quando il bersaglio sta utilizzando la tecnologia wireless. Questo è di solito un sistema basato computer portatile che impersona una stazione di WiFi o 3G di base per catturare i sistemi di destinazione e le richieste dei relè a monte a Internet. Una volta che il target sono i sistemi in rete, il sistema funziona quindi come *un'iniezione proxy* o come *monitor a monte* al fine di infiltrarsi o monitorare il sistema di destinazione.
- Una *chiave USB* precaricata con l'untore del malware può essere dato o è sceso al sito di destinazione.

Agenti Cyber-raccolta sono generalmente installati da software di consegna payload costruito utilizzando zero-day attacchi e consegnati tramite unità USB infette, allegati e-mail o siti Web dannosi. Stato sponsorizzato cyber-collezioni sforzi hanno utilizzato certificati ufficiali del sistema operativo al posto di basarsi su vulnerabilità di sicurezza. Nell'operazione Fiamma, Microsoft afferma che il certificato Microsoft ha utilizzato per impersonare un Windows Update è stato forgiato; Tuttavia, alcuni esperti ritengono che potrebbe essere stata acquisita attraverso HUMINT sforzi.

Guerra cibernetica

Da Wikipedia, l'enciclopedia libera.

Il termine **guerra cibernetica**[1] (noto nell'ambito operativo militare del mondo anglofono come *cyberwarfare*) è l'insieme delle attività di preparazione e conduzione di operazioni di contrasto nello spazio cibernetico. Si può tradurre nell'intercettazione, nell'alterazione e nella distruzione dell'informazione e dei sistemi di comunicazione nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione.

Indice

Dominio cibernetico

A livello strategico lo spazio cibernetico è considerato il più recente ambiente di guerra ovvero il quinto dominio dopo terra, mare, cielo e spazio.

A livello geopolitico gli Stati Uniti detengono il primato su questo ambiente dato dal possesso delle principali aziende tecnologiche di portata planetaria, unito al relativo potenziale di intercettazione e attacco e alla disponibilità di gran parte delle infrastrutture della connessione (server, cavi, centri di stoccaggio dati, eccetera).

Anche possedendo questi vantaggi logistici lo spazio cibernetico per sua conformazione offre l'occasione di sfruttare le enormi ignote vastità per sfidare avversari di forze impari, in modi altrimenti inimmaginabili negli altri domini. Per sua natura le battaglie in questo dominio sono svolte principalmente da agenzie di servizi segreti e raramente si riesce a individuare gli attori responsabili ed ancora più difficilmente poterli giudicare in base a una giurisdizione univoca. La pervasività odierna della Rete nella vita dei singoli cittadini come nelle infrastrutture dove ormai è diventata indispensabile al loro funzionamento, se da un lato comporta un esteso controllo centralizzato di contro presenta una fragilità intrinseca del sistema che può essere infiltrato in qualsiasi momento e danneggiato anche nei punti più vitali nonostante tutte le precauzioni[2].

Tipi di attacchi

Esistono molte metodologie di attacco nella guerra cibernetica.

- **Attacco a infrastrutture critiche**: i servizi energetici, idrici, di combustibili, di comunicazioni, commerciali, dei trasporti e militari sono tutti potenziali obiettivi di questo genere di attacchi.
- **Vandalismo web**: attacchi volti a modificare indebitamente pagine web, chiamati in gergo *deface*, o a rendere temporaneamente inagibili i server (attacchi denial-of-service). Normalmente queste aggressioni sono veloci e non provocano grandi danni se l'attaccante non riesce ad avere un accesso con privilegi abbastanza elevati da permettergli di intercettare, rubare o eliminare i dati presenti sul sistema colpito.
- **Intralcio alle apparecchiature** (*equipment disruption*): le attività militari che utilizzano computer e satelliti per coordinarsi sono potenziali vittime di questi attacchi. Ordini e comunicazioni possono essere intercettati o sostituiti, mettendo a rischio le operazioni.
- **Raccolta dati**: informazioni riservate ma non adeguatamente protette possono essere intercettate e modificate, rendendo possibile lo spionaggio.
- **Propaganda**: messaggi politici che possono essere spediti o resi disponibili in rete a scopo di coordinamento o per la guerra psicologica, fake news.

Attacchi conosciuti

- Gli Stati Uniti d'America hanno ammesso di essere stati sotto attacco da parte di diversi Stati, ad esempio Cina e Russia. I due attacchi più famosi sono passati alla storia con i nomi di Titan Rain e Moonlight Maze.[3]
- Attacco alla centrale atomica dell'Iran da parte degli Stati Uniti d'America: operazione Stuxnet.

Regole base

Le regole base della cyberwarfare sono:

- minimizzare la spesa di capitali e di energie produttive e operative;
- sfruttare appieno tecnologie che agevolino le attività investigative e di acquisizione di dati, l'elaborazione di questi ultimi e la successiva distribuzione dei risultati ai comandanti delle unità operative;
- ottimizzare al massimo le comunicazioni tattiche, i sistemi di posizionamento e l'identificazione amico-nemico (IFF - "*Identification Friend or Foe*").

Organizzazione

Con il cyberwarfare si conosce un radicale riassetto delle concezioni organizzative militari. Le tradizionali strutture gerarchiche si vedono progressivamente soppiantate da sistemi a rete, con nuovi ruoli di complementarità e integrazione. Si fanno così spazio entità operative caratterizzate da:

- ridotta consistenza numerica;
- elevato livello di supporto tecnologico;
- efficacia assoluta.

Controspionaggio cyberspaziale

Il controspionaggio cyberspaziale è l'insieme delle misure atte a identificare, penetrare o neutralizzare operazioni straniere che usano i mezzi cyber come metodologie di attacco primario, così come gli sforzi dei servizi stranieri di intelligence che, attraverso l'uso di metodi tradizionali, cercano di portare avanti attacchi di cyberwarfare[4].

Note

1. **^** Cfr. in Riccardo Busetto, *Il dizionario militare: dizionario enciclopedico del lessico militare*, Bologna, 2004, Zanichelli, ISBN 9788808089373
2. **^** Limes,*La rete a stelle e strisce. Cyberwarfare, dove nessuno domina*, GEDI, n 10, 2018, ISSN 2465-1494

3. ^ (EN) Reuters: L'U.S. Air Force si prepara a combattere nel cyberspazio (http://www.propagandamatrix.com/articles/november2006/031106_b_cyberspace.htm) Archiviato (https://web.archive.org/web/20070221032158/http://www.propagandamatrix.com/articles/november2006/031106_b_cyberspace.htm) il 21 febbraio 2007 in Internet Archive.
4. ^ (EN) Controspionaggio cibernetico degli Stati Uniti (http://ncix.gov/issues/cyber/index.php) Archiviato (https://web.archive.org/web/20150402154318/http://ncix.gov/issues/cyber/index.php) il 2 aprile 2015 in Internet Archive.

Bibliografia

- Maddalena Oliva, *Fuori Fuoco. L'arte della guerra e il suo racconto*, Bologna, Odoya 2008. ISBN 978-88-6288-003-9.
- Daniel Ventre, *La guerre de l'information*, Hermès-Lavoisier, Sept.2007.
- Daniel Ventre, *Information Warfare*, Wiley-ISTE, Nov. 2009.
- Daniel Ventre, *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Hermès-Lavoisier, Sept.2010.
- Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, Hermès-Lavoisier, April 2011.
- Daniel Ventre, *Cyberwar and Information Warfare*, Wiley-ISTE, July 2011.
- Daniel Ventre, *Cyberattaque et Cyberdéfense*, Hermès Lavoisier, August 2011.

Voci correlate

- Sicurezza informatica
- Armi a impulso elettromagnetico
- Guerra elettronica
- ELINT
- Intelligence
- High Energy Radio Frequency weapons (HERF)
- SIGINT
- PRISM (programma di sorveglianza)
- Operazione Aurora
- Hacker
- Stuxnet
- Attacco informatico
- Network-centric warfare

Altri progetti

- Wikimedia Commons (https://commons.wikimedia.org/wiki/?uselang=it) contiene immagini o altri file su **guerra cibernetica (https://commons.wikimedia.org/wiki/Category:Cyberwarfare?uselang=it)**

Collegamenti esterni

- *Sistema di informazione per la sicurezza della Repubblica*, su *sicurezzanazionale.gov.it*.
- *DPCM 27 gennaio 2014 – Strategia nazionale per la sicurezza cibernetica*, su *sicurezzanazionale.gov.it*.
- *CyberDifesa.it - notizie sulla guerra cibernetica*, su *cyberdifesa.it*.
- *Esercitazioni di "Cyber Defence" per la Difesa*, su *difesa.it*.

MOTHERBOARD
TECH BY VICE

La guida di Motherboard per non farsi hackerare

Ecco le cose principali da fare per mettere al sicuro noi stessi e i nostri dati.

Di **Lorenzo Franceschi-Bicchierai e Joseph Cox**

31 agosto 2016, 11:32am

Internet può essere un posto davvero spaventoso, dove un hacker rubano **centinaia di milioni** di **password** in un colpo solo e un altro causare, a piacere, **un blackout su vasta scala**.il futuro non promette molto meglio: **disastri reali causati da apparecchiature connesse a internet**, r**obot domestici che possono uccidere**, **portatili volanti** e **il rischio concreto che un hacker malintenzionato possa aver accesso ai tuoi dati genetici**.

La minaccia è una vostra ex che temete possa accedere al vostro account Facebook? Allora assicurarvi che non conosca la password del suddetto account Facebook, beh, potrebbe essere un buon inizio. (Non condividete mai le passowrd importanti con nessuno, non importa di chi si tratti; se condividete un account Netflix con qualcuno assicuratevi di non riutilizzare *mai* quella password altrove.) State cercando di tenere alla larga qualche truffatore opportunista, ché non riesca a raccogliere troppe informazioni personali sul vostro conto? D'accordo, fate bene attenzione a cosa pubblicate sui social. Ah, usate sempre l'autenticazione a due fattori (approfondiremo più tardi) ogni qual volta sia disponibile. Sempre.

Anche sovrastimare la propria minaccia può generare effetti paradossali, comunque: se cominciate a usare sistemi operativi personalizzati, macchine vertuali o qualsiasi tecnica avanzata dove non necessario (o senza saperle davvero usare) potreste fare qualche danno. Nel migliore dei casi operazioni semplici potrebbero diventare estremamente più lunghe; nel peggiore dei casi, invece, i vostri gadget potrebbero ipnotizzarci in un falso senso di sicurezza, mentre tralasciate le cose davvero importanti.

Con questo in mente, ecco i promessi, semplici, consigli per prevenire alcune delle più comuni minacce online.

RICORDATEVI DI AGGIORNARE LE APP

Forse la cosa più elementare e parimenti importanti che possiate fare, per proteggervi, è usare software sempre aggiornato. Questo significa utilizzare una versione aggiornata, appunto, di qualsiasi sistema operativo utiliziate e aggiornare sempre tanto le vostre app sullo smartphone, quando, in generale, i vostri software. Tenete a mente, anche, che non dovete necessariamente utilizzare l'ultima versione del vostro sistema operativo come, per esempio, Windows 10 (in certi casi alcune versioni passate di un sistema operativo continuano a ricevere supporto e aggiornamento. Purtroppo non è più il caso di **Windows XP**, no, e quindi smettetela subito di usarlo)

Prima lezione della guida di Motherboard alla sicurezza informatica: aggiornate, aggiornate, aggiornate, patchate, patchate, patchate.

Alcuni dei più comuni cyberattacchi sfruttano le vulnerabilità del software datato, che sia un browser o un lettore di PDF. Tenendo tutto aggiornato per benino abbassate di molto le vostre possibilità di essere la prossima vittima di ransomware, per esempio (una forma di hack che prevede il pagamento di un vero e proprio riscatto, entro un certo tempo, pena la salute del vostro computer o dei vostri dati)

PASSWORD

Abbiamo tutti troppe password da tenere a mente ed è proprio il motivo per cui la maggior parte delle persone riutilizza la stessa ovunque. E, **anche se apparentemente i nostri cervelli sono piuttosto efficienti a ricordare le pasword**, è quasi impossibile ricordarsi venti o più password forti, prodotte come si deve.

La buona notizia è che la soluzione al problema è già là fuori: i password manager. Un password manager è un software che genera e memorizza le password al postro vostro e sì, semplifica di molto la vita. Se usate un manager tutto ciò che dovrete ricordare è una singola password, il più complessa possibile, che sblocchi la cassaforte virtuale che contiene tutte le altre.

Intuitivamente, potreste pensare sia poco saggio salvare tutte le vostre password sul computer, per quanto complesse. E se un hacker si facesse largo? Non è certamente meglio me le tenga tutte per me, stipate nella zucca? Beh, no: il rischio che qualcuno si approfitti di una password riciclata su più siti è molto, molto più elevato che qualche hacker, dalle abilità davvero sofisticate, oltretutto, riesca a caricare un malware particolarmente sofisticato sul vostro computer e accedere al manager. Ancora, si tratta di capire cosa vi minaccia.

Quindi, per piacere, usate **uno dei molti password manager disponibili**. Non esiste un solo buon motivo per non farlo. Vi metterà più al sicuro—e noi con voi. E poi, insomma, renderà la vostra vita addirittura più confortevole.

TWO-FACTOR AUTHENTICATION

Avere un'unica password forte è un buon inizio, ma anche queste possono essere sottratte. Per questo, quantomeno per i vostri account più importanti (la vostra mail principale, Facebook e Twitter, per esempio) potreste aggiungere uno strato ulteriore di sicurezza attivando quella che è nota come 2FA, autenticazione a due fattori, o passi.

Attivandola avrete bisogno di qualcosa di più della sola password, per connettervi a questi account. Di solito, un codice numerico mandato al vostro cellulare o potrebbe essere un codice creato da qualche applicazione ad hoc (che è molto comodo quando avete urgenza di connettervi a qualcosa, ma il telefono non ha campo)

Si discute molto, ultimamente, su come i cellulari potrebbero in realtà non essere adatti alla 2FA. **Il numero telefonico dell'attivista Deray McKesson è stato dirottato**, il che signifca che l'hacker in questione aveva accesso ai codici di sicurezza a protezione dei vari account, semplicemente facendoseli spedire. E l'istituto nazionale degli standard e della tecnologia" (NIST), un ramo del governo degli Stati Uniti che compila le linee guida per ogni genere di misure, inclusa la sicurezza, ha recentemente scoraggiato l'uso della 2FA basata su SMS.

L'attacco ai danni di Deray era molto semplice e poco high tech: l'hacker è riuscito a convincere la compagnia telefonica a inviargli una copia della SIM della vittima. È difficile difendersi da questo genere di cose, oltretutto gli SMS presentano altre criticità ed esistono altri modi per ottenere quei codici dal momento che un messaggio può, in linea teorica, essere intercettato da qualcuno che faccia leva su alcune vulnerabilità nella dorsale dell'operatore che gestisce le vostre conversazioni. C'è anche la possibilità di utilizzre un IMSI-catcher, altresì noto come **Stingray**, per intercettare direttamente le comunicazioni e, ovviamente, anche i codici di verifica per l'autenticazione a due fattori.

A differenza di ottenere una nuova SIM, però, questi attacchi non sono per niente rudimentali, non solo perché richiedono strumenti costosi e specifici: proprio come lo Stingray, per esempio. Quindi, realisticamente, per la maggior parte delle persone nel mondo la 2FA via SMS è una misura sufficientemente robusta e adatta al suo compito: aggiungere un ulteriore strato di sicurezza alla propria password che potrebbe essere rubata.

Come anticipato, se il sito lo prevede e ve lo permette, utilizzare un'altra opzione di 2FA (non basate su SMS, ma su delle app di autenticazione (per esempio, **Google Authenticator**) o addirittura assicurarvi un token fisico come **Yubikey** (simili a quelli associati a molte carte di credito). Se queste opzioni sono previste vi consigliamo caldamente di adottarle, ma sarebbe davvero ingeneroso denigrare la buona 2FA via SMS, spercialmente se non siete sotto attacco.

La 2FA è un grande modo di rendere quasi impossibile al cybercriminale medio accedere ai vostri dati. Qui potete controllare tutti i siti che offrono il servizio e le guide su come attivarli.

DOs & DON'Ts

Non utilizzate Flash: Flash è storicamente uno dei software più insicuri che abbia popolato il vostro computer. Gli hacker adorano Flash perché ha più buchi di un formaggio svizzero. La buona notizia è che la gran parte del web ha mollato Flash quindi non ne avete più davvero bisogno, senza rinunciare a un'esperienza di navigazione ricca e piacevole. Quindi, sì, prendete in considerazione di esorcizzarlo dal vostro computer una volta per tutte, o almeno di modificare le impostazioni relative del vostro browser perché vi chieda conferma ogni volta che dovrete aprire un contenuto Flash.

Utilizzate un antivirus: sì, immaginiamo ne abbiate già sentito parlare. Ma resta ancora vero (generalmente). In effettii antivirus, piuttosto

ironicamente, **sono pieni di falle di sicurezza**, ma è del tutto probabile non siate così importanti da essere sotto attacco di un team di hacker nazionali e crittologi. Avere un antivirus rimane una buona idea. Resta il fatto, e non si tratta di paranoia, che nel 2016 avete bisogno di *più* di un antivirus per essere al sicuro.

Utilizzate alcuni semplici plugin di sicurezza: A volte, tutto ciò di cui ha bisogno un hacker per pwnarvi è di attirarti sul sito giusto—ovviamente farcito di malware. Per questo vale la pena usare alcuni semplici plugin come **adblockers**, che vi protegge dalla **pubblicità tossica**. (naturalmente noi di Motherboard avremmo piacere mettiate in whitelist il sito, perché i proventi pubblicitari pagano le nostre bollette)

Un altro plugin utile è **HTTPS-Everywhere**, che forza di default la connessione criptata per tutti quei siti (molti) che lo permettono. Non vi salverà se il sito che state visitando contiene malware, ma in alcuni casi, gli hacker proveranno a re-indirizzarvi su una versione falsa dello stesso sito (se ne esiste una versione criptata) e il plugin vi proteggerà dai tentativi di instrusione nella vostra connessione.

Utilizzare una VPN: se state accedendo a internet da uno spazio pubblico che sia Starbucks, l'aeroporto o addirittura **un appartamento affittato su Airbnb** state condividendo quella connessione con qualcuno che non conoscete. E se un malintenzionato è presente sul network può avere accesso ai vostri dati, compromettere la connessione o, addirittura, danneggiare il computer.

Cercate di non sovraesporvi: Le persone amano condividere sui social qualsiasi aspetto della propria vita. Ma per piacere, vi spplichiamo, non postate su Twitter una foto della vostra carta di credito o cose di questo tipo. Più in generale, è una buona idea capire che un post su un social è spesso un post che chiunque su internet può leggere, che i vostri profili sono visitabili e spesso pubblici e che con un po' di impegno potrebbe anche

scoprire l'indirizzo di casa vostra o i vostri percorsi su siti come Strava, un network per runner e ciclisti.

Le informazioni personali come il vostro indirizzo o le scuole che avete frequentato, a loro volta, possono ricondurre a un gran numero di altre informazioni tramite **ingegneria sociale**. Più informazioni personali sono in possesso dell'hacker e più è probabile riesca a ottenere l'accesso ai vostri accounts. Tenendo questo ben in mente, potreste considerare di aumentare i settaggi relativi alla privacy ovunque possibile.

Non aprite gli allegati mail a cuor leggero: per decenni, i cybercriminali hanno nascosto malware in allegati come file di testo o PDF. Gli antivirus qualche volta intercettano questo tipo di minacce, ma è molto meglio usare il semplice buon senso: non aprite allegati (né cliccate su link) di persone che non conoscete o che non stavate aspettando. E se volete proprio farlo--non potete proprio resistere--fatelo con precauzione, per esempio aprendo l'allegato all'interno di Chrome, senza scaricare effettivamente i file. Ancora meglio: salvate il file su Google Drive e poi apritelo all'interno di Drive; il motivo per cui è un'idea ancora migliore è che in questo modo il file sarà aperto da Google e non dal vostro computer.

Disabilitate le macro: un hacker può utilizzare le macro di Microsoft Office per diffondere malware nel vostro computer. È un vecchio trucco, ma sta **tornando di moda**. Disabilitatele e basta.

Fate regolari backup dei vostri file: sì, come per l'antivirus non stiamo dando un grande suggerimento, ma se siete preoccupati che un hacker possa compromettere i vostri file (per esempio in un caso di **ransomware**) ecco che averne uno o più backup diventa davvero una buona idea. Idealmente, fate i vostri backup sconnessi da internet, utilizzare hard disk esterni così che anche in caso di ransomware il contenuto dei backup non potrà fisicamente essere infettato.

Sorvegliati di tutto il mondo, unitevi!

Oliviero Ponte Di Pino (/autore/Oliviero-Ponte-Di-Pino)

Secondo Comscore, su internet la visualizzazione di una pagina dura in media 26 secondi. Il 99,8 per cento delle visualizzazioni dura meno di dieci minuti. Leggere questo articolo fino in fondo sarebbe un comportamento marginale, residuale. Per gli algoritmi è irrilevante, anomalo, forse addirittura patologico.
La logica dei signori della rete è impeccabile, efficientissima. Ma questa logica ci sta fregando, o forse ci ha già fregato. Perché accanto alla rete in cui navighiamo inconsapevoli, sono state create altre reti. Non le vediamo e proprio per questo sono ancora più importanti.

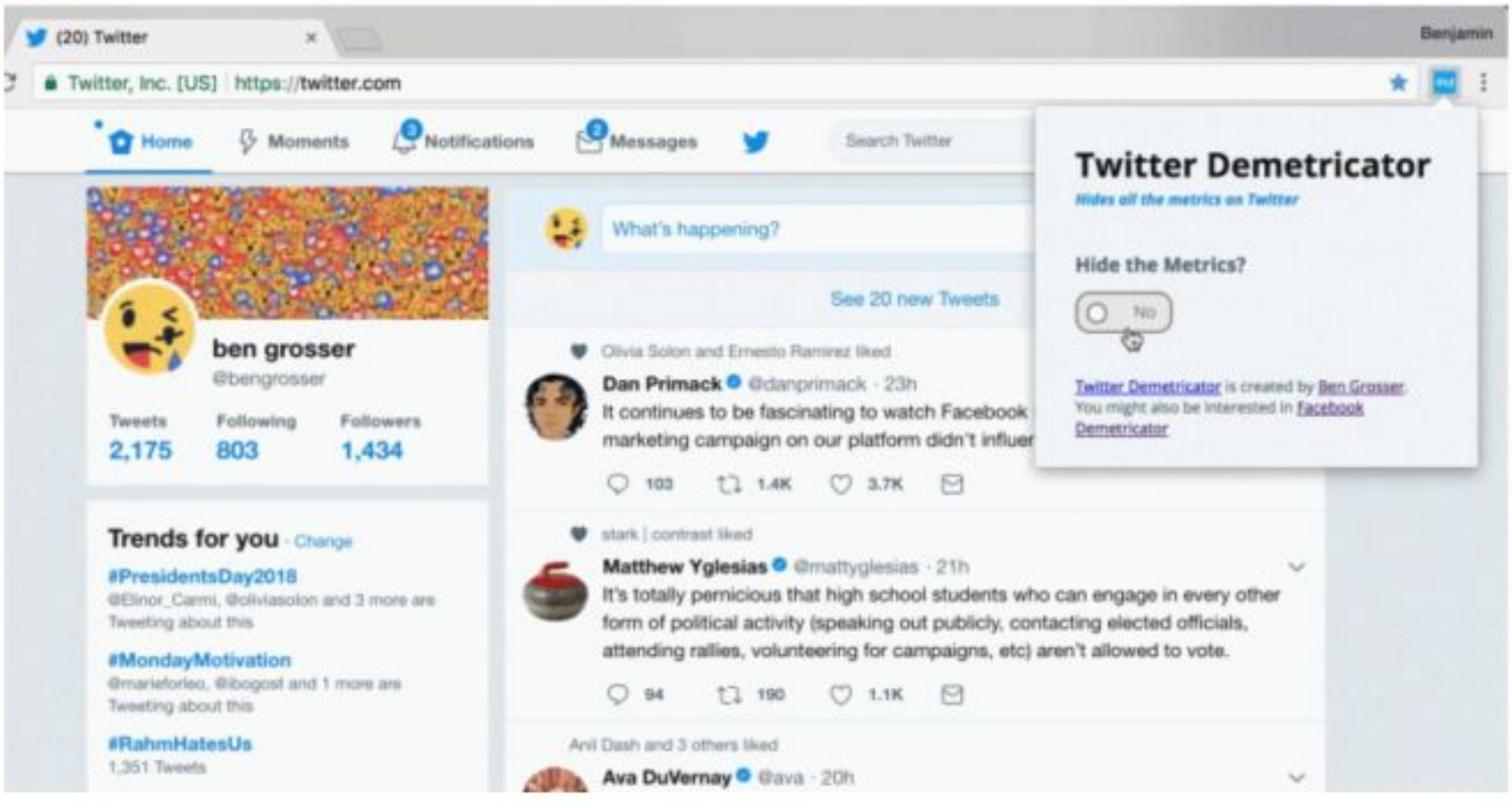
I due internet secondo Matthew Hindman

Esistono due internet, secondo Matthew Hindman, autore di *La trappola di internet* (traduzione di Daniele A. Gewurz, Einaudi, Torino, 2019, 286 pagine, 22 €). La prima è "l'internet 'di cui tutti sanno', che sta democratizzando la comunicazione e la vita economica". L'aveva profetizzata nel 1996 John Perry Barlow in *A declaration of independence of cyberspace* (1996): la rete sarà immune a qualsiasi regola e completamente separata dal "Mondo Industriale", destinata a diventare "la nuova casa della Mente", in cui "qualunque cosa la mente umana possa creare può essere riprodotta e distribuita all'infinito senza alcun costo. Il trasferimento globale del pensiero non richiede più le vostre fabbriche".
Poi c'è l'internet reale, dove "un terzo di tutte le visite web va alle prime dieci aziende" e che "consente a due aziende di controllare più della metà delle entrate pubblicitarie online" (p. 201) e il 70 per cento della pubblicità online negli USA.
Hindman, professore associato di Media and Public Affairs e consulente della Federal Communication Commission statunitense, ha analizzato e modellizzato l'evoluzione dell'economia della rete. Le sue conclusioni sono drastiche. Il fattore decisivo per avere successo online è la *stickiness*, ovvero la capacità di un sito di attrarre e conservare i visitatori. L'obiettivo è quello che gli economisti chiamano *lock in*, che si realizza quando i costi di passaggio a un altro fornitore superano i possibili benefici.
L'errore di prospettiva è stato pensare che con il World Wide Web i costi di distribuzione delle informazioni si sarebbero azzerati: si sono solo spostati dal mondo fisico a quello virtuale. Non servono più camion, navi o aerei e fattorini, ma le *server farms* con migliaia di computer che inghiottono giganteschi flussi di energia, e sistemi di commutazione con una larghezza di banda di diversi terabyte al secondo, progettati e gestiti da un'aristocrazia di ingegneri del software. Il tutto affinato da continui e costosi test A/B per valutare le soluzioni migliori anche nei dettagli: dai titoli più efficaci ai pixel di un carattere o a una sfumatura di colore. Per quanto riguarda le notizie, la

quantità vale più della qualità: "i consumatori leggono una gran quantità di contenuti mediocri e poco curati" (p. 93). Meglio raffiche di spazzatura che reportage documentati e inchieste validate dal *fact checking*, meglio il gattino in bottiglia o il pettegolezzo sexy della recensione.

Il metodo di raccomandazione/filtraggio (per consigliare un libro su Amazon, una pagina su Google, un film su Netflix, un post su Facebook, un ristorante su Tripadvisor) si è via via affinato.
Inizialmente a essere privilegiati erano i contenuti *più popolari*. In una seconda fase è intervenuto il *filtraggio collaborativo*: "via via che il sistema registra una quantità maggiore di dati sui clic, le raccomandazioni si basano sempre più sul comportamento passato degli utenti e degli interessi dimostrati" (p. 69). Ha fatto progressi anche la gestione dei *contenuti*, che usa "l'analisi del testo per abbinare gli utenti con i tipi di articoli che hanno apprezzato in passato" (p. 68). Le strategie più efficaci utilizzano un modello ibrido, che combina questi tre approcci.
Nella lotta per la *stickiness* un piccolo vantaggio porta nel lungo periodo a "enormi differenze nel numero di visitatori" (p. 61). Le economie di scala favoriscono le imprese maggiori e creano monopoli, esattamente come era successo alla fine dell'Ottocento con i *robber barons*, gli odiati signori dell'acciaio e delle ferrovie. In rete trionfano i giganti. Oggi "internet non è affatto un ecosistema, ma un paio di monoculture commerciali" (p. 221)

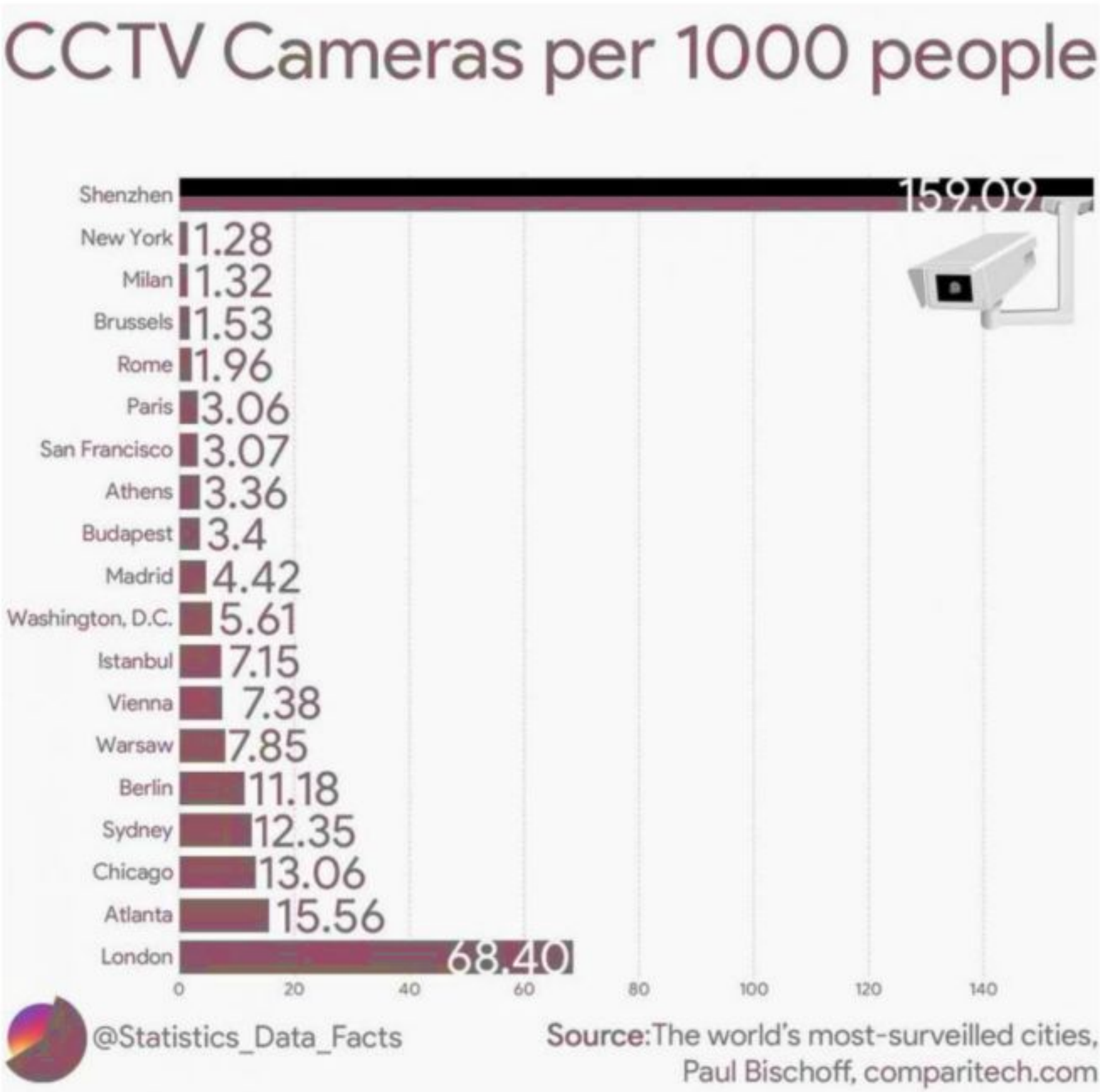
Contro chi continua a considerare la rete il Paradiso dell'innocenza egualitaria, le analisi di Hindman dimostrano che negli USA, mentre i giornali locali "di carta", una delle spine dorsali della democrazia americana, chiudono uno dopo l'altro, le nuove testate online restano marginali.
Oltre a sottrarre pubblicità ai media tradizionali, Facebook e Google hanno affinato meccanismi "personalizzati" che promettono agli inserzionisti un'efficacia molto maggiore. Gli algoritmi usati dai giganti dei web funzionano per sei ordini di ragioni:
"i sistemi di raccomandazione possono aumentare notevolmente il pubblico";
e "favoriscono le aziende digitali con ampi contenuti";
"avvantaggiano le imprese con hardware migliore e personale più qualificato";
e "favoriscono le imprese con più dati", ovvero "i siti più popolari e più frequentati";
"i sistemi di personalizzazione promuovono il *lock-in*";
"i sistemi di suggerimenti incoraggiano la concentrazione del pubblico" (pp. 75-77).



Risultato? Se un sito raddoppia il suo pubblico, le sue entrate pubblicitarie saranno più del doppio (e i profitti cresceranno grazie alle economie di scala). Oltretutto "il pubblico dei grandi siti è molto più costante di quello dei siti più piccoli", anche se "le fluttuazioni quotidiane del traffico rendono stabile

la *struttura* del web" nel suo insieme. Ignoriamo se tra due o cinque anni Doppiozero avrà più o meno visite di oggi, ma sappiamo quante visite avrà il sito che occupa la sua posizione nella classifica del traffico. E la top ten cambierà di poco, a meno di clamorosi fallimenti (p. 106).

C'è un'altra costante, secondo Hindman: "la percentuale di pubblico che cerca le notizie rimane stabile da vent'anni al 3 per cento circa" (p. 203), limitato da una feroce *competizione per l'attenzione*. La conseguenza politica è immediata: "La nuova organizzazione politica basata sui dati beneficia di economie di scala enormi. La fortissima concorrenza per l'attenzione fa sì che sia ancora più difficile per gli attivisti su piccola scala farsi notare" (p. 208). Le vittorie elettorali di Barack Obama, Donald Trump e Boris Johnson, basate sui big data e sui meccanismi portati alla luce dallo scandalo su Cambridge Analytica, sembrano confermare questa ipotesi, anche se il successo planetario dei Fridays for Future di Greta e l'epidemia delle sardine in Italia lascia qualche speranza (anche se per certi aspetti questi due movimenti restano in una sfera pre-politica).

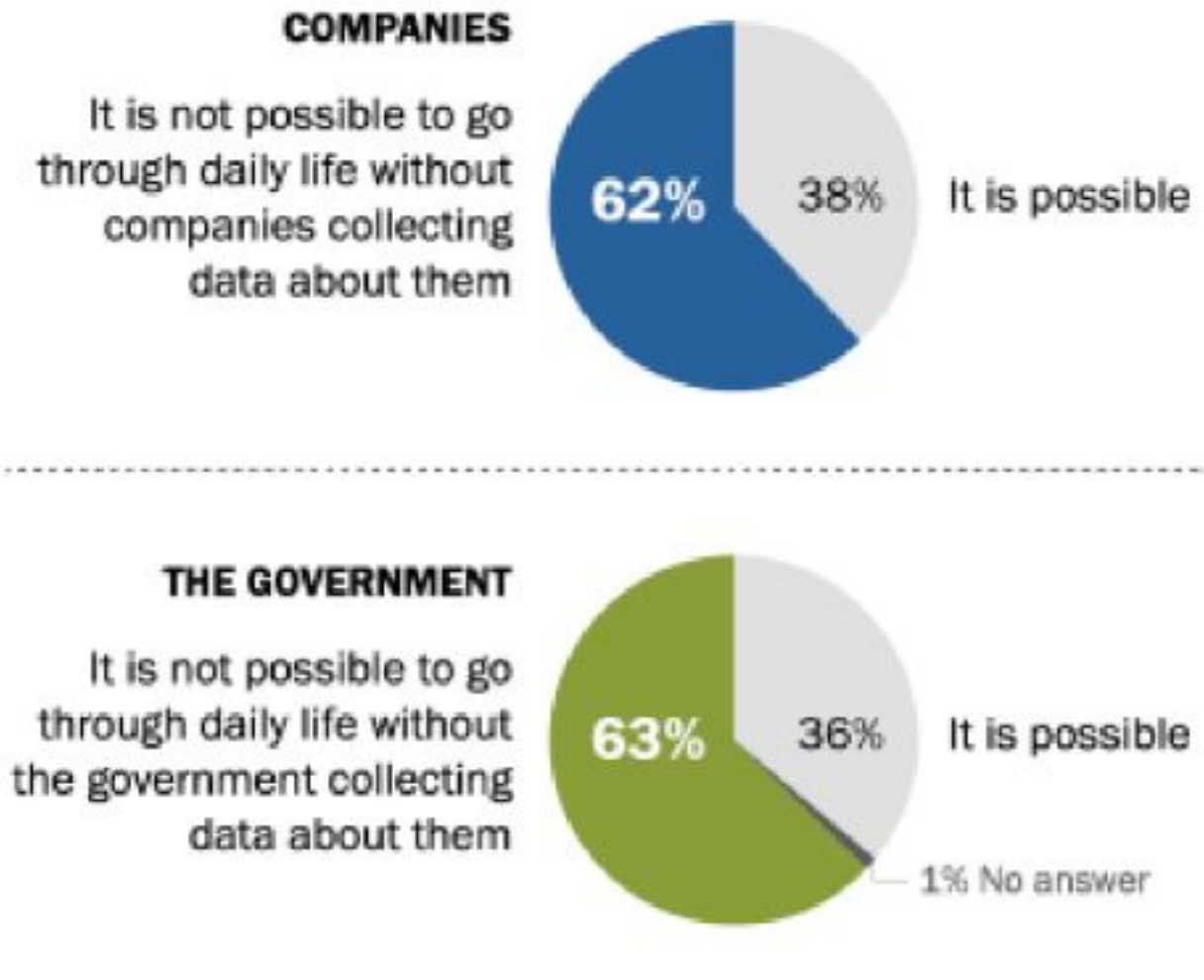


I due internet secondo Shoshana Zuboff

Esistono due internet anche per Shoshana Zuboff, professoressa alla Harvard Business School e autrice del poderoso *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (traduzione di Paolo Bassotti, Luiss, Roma, 2019, 622 pagine, 25 €).
Il "primo testo" è quello che vediamo (o meglio, quello che potremmo vedere): sono i contenuti che ciascuno di noi pubblica (gratuitamente) sui social e in rete, e le nostre interazioni di tutti i generi ormai digitalizzate, per esempio quando facciamo la spesa, paghiamo una bolletta o andiamo dal medico. Come ha spiegato Hal Varian, a lungo *chief economist* di Google, "al giorno d'oggi c'è un computer di mezzo in quasi ogni transazione [...] e ora che sono disponibili, tali computer vengono utilizzati in tanti altri modi" (p. 74). In particolare servono per:
l'estrazione e l'analisi dei dati;
le nuove forme contrattuali dovute a un miglior monitoraggio (pensate alle assicurazioni...);
la personalizzazione e customizzazione;
gli esperimenti continui (ovviamente a insaputa delle cavie, cioè noi).
Questo primo testo – la nostra impronta digitale – è talmente gigantesco che nessun cittadino è in grado di vedere le informazioni che contiene (e men che meno di controllarle ed eventualmente farle correggere). Oltretutto molte di queste informazioni sono state raccolte a nostra insaputa, in violazione di qualunque principio di privacy e senza alcuna possibilità di controllo: "il diritto alla privacy, alla conoscenza e al suo uso è stato usurpato da un mercato aggressivo che ritiene di poter gestire unilateralmente le esperienze delle persone e le conoscenze da esse ricavate" (p. 17).
In una prima fase questi dati venivano utilizzati a favore dell'utente, per garantirgli un servizio più efficace. Ma a partire dal 2002, in seguito allo scoppio della bolla di internet e all'imperativo di massimizzare i profitti, questo *surplus comportamentale* è stato dirottato a favore degli inserzionisti: le informazioni (espropriate agli utenti) hanno prodotto un advertising mirato, attraverso forme di *user profile information* sempre più accurate (grazie alle economie di scala e agli effetti di rete), in grado di "inferire e dedurre i pensieri, le emozioni, le intenzioni e gli interessi di individui e gruppi" (p. 91) con crescente precisione.
Oggi Google estrae surplus comportamentale da "qualunque elemento del mondo digitale: ricerche, email, messaggi, foto, canzoni, chat, video, luoghi, schemi comunicativi, atteggiamenti, preferenze, interessi, volti, emozioni, malattie, social network, acquisti e così via" (p. 139). Ma non è solo Google. L'estrazione è sistematica, ossessiva, invasiva. Già nel 2015 "chiunque avesse visitato i 100 siti più popolari aveva raccolto più di 6000 cookie nel proprio computer, l'83 per cento dei quali appartenenti a parti terze non correlate al sito visitato" (p. 146).

Roughly six-in-ten Americans believe it is not possible to go through daily life without having their data collected

% of U.S. adults who say ...



Note: Respondents were randomly assigned to answer a question about whether they think it is possible to go about daily life without having personal information collected from them by "companies" or "the government."
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

PEW RESEARCH CENTER

Secondo Zuboff, ci siamo comportati come gli indigeni ai quali i colonizzatori facevano firmare contratti che non potevano capire, cedendo la proprietà delle terre in cambio di collanine e perle di vetro. In questo modo la nostra vita privata, la nostra esperienza e la nostra intimità ci sono state sottratte, in un "ciclo dell'esproprio" incessantemente ripetuto, basato sull'*incursione* dei vari dispositivi nelle nostre vite, sulla *assuefazione* al nuovo scenario, su un *adattamento* minimo in caso di eventuali resistenze e contestazioni, e sul *reindirizzamento* verso nuovi obiettivi. Senza nemmeno darci le perline...
I terreni da colonizzare e sfruttare si stanno moltiplicando.
Lo spazio pubblico è controllato dalle telecamere di sorveglianza (e presto dai droni) che, con i meccanismi di riconoscimento facciale, sono ormai in grado di ricostruire i movimenti di veicoli e persone (vedi Madhumita Murgia, *Who's using your face? The ugly truth about facial recognition* (https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e), "Financial Times", 18

settembre 2019, e Silvia Bottani, *L'occhio della macchina* (https://www.doppiozero.com/materiali/locchio-della-macchina)). Anche le nuove automobili intelligenti sono una miniera di dati.
Nelle nostre case l'IoT, l'*internet of things*, sta connettendo alla rete elettrodomestici, abiti, giocattoli... Assistenti personali come Alexa, Cortana e Siri convivono già con il 25 per cento degli americani adulti e trasmettono un costante flusso di informazioni, elaborate senza alcun controllo da parte dell'utente.

Ma non basta. Il "primo testo" fornisce le materie prime per un secondo testo, un "testo ombra" ancora più invisibile e gigantesco, tanto complesso e dinamico che può essere gestito solo dagli algoritmi. Qui i contenuti hanno poca importanza: contano le relazioni che le macchine riescono a estrarre dalla "materia prima", cioè gli utenti di internet. Come hanno scoperto nel 2011 tre ricercatori dell'Università del Maryland, "i semplici metadata (...) sono più utili e predittivi dei dati grezzi originali" (p. 287). I *dati di scarto* che intasavano i server di Google e degli altri giganti del web sono diventati la più preziosa delle merci.

Published: December 14, 2013

Face to Anti-Face

ADAM HARVEY

Adam Harvey is a Brooklyn-based artist whose work addresses the impact of surveillance technologies.

Next year the Janus program, an initiative run by the director of national intelligence, will begin to collect photographs of people's faces from social media websites and public video feeds. Machines will then use powerful algorithms to pair those photos with existing biometric profiles.

The Janus program isn't alone: Facial-recognition technology is quickly becoming a mainstay of commercial and government surveillance systems. While it can provide benefits in automation and security, it is also a threat to privacy. Sophisticated algorithms can already extract information about your gender, age and even mood from a single image, and then link those physical attributes to commercial or government databases.

This powerful surveillance technology is cheap, ubiquitous and unregulated.

My project, CV Dazzle, explores how fashion can be used as camouflage from face-detection technology, the first step in automated face recognition. The name is derived from a type of World War I naval camouflage called Dazzle, which used cubist-inspired designs to break apart the visual continuity of a battleship and conceal its orientation and size. Likewise, CV Dazzle uses avant-garde hairstyling and makeup designs to break apart the continuity of a face. Since facial-recognition algorithms rely on the identification and spatial relationship of key facial features, like symmetry and tonal contours, one can block detection by creating an "anti-face."

Camouflaged Fashion

This design combines unconventional hairstyling and makeup to create an anti-face, an attempt to block facial recognition software.

USE TONAL INVERSE

Some algorithms will analyze gradations in skin tone and texture. This process helps locate the facial region, but it relies on assumptions about what typical facial features look like. To confuse this process, use hair or makeup that contrasts with your skin tone and apply makeup in unusual tones and directions: light colors on dark skin, dark colors on light skin.

CREATE ASYMMETRY

Facial-recognition algorithms expect symmetry between the left and right sides of the face. By developing an asymmetrical look, you may decrease your probability of being detected.

CONCEAL THE NOSE BRIDGE

Some algorithms rely on the nose bridge area as a key facial marker. Use hairstyling or fashion accessories to conceal the area above the nose and between the eyes.

Per capire che cosa pensiamo, che cosa desideriamo, qual è il nostro stato emotivo, è più utile – nel caso di Instagram, per esempio – guardare quali filtri usiamo, quanti post facciamo (e quando), quanti cuoricini mettiamo (e a chi), e chi mette i like sui nostri post (e quanti e quando). Quel che si vede nelle immagini è relativamente irrilevante, con buona pace di chi proclamava che "in rete il contenuto è re". Per questo i social network e i motori di ricerca non sono interessati a eliminare le *fake news*: al centro dell'attenzione ci sono le azioni e le relazioni, e le *fake news* sono efficacissime nel generare "traffico".
Il "secondo testo", il nostro DNA digitale, viene estratto da quello ci è stato massicciamente sottratto senza che ce ne accorgessimo e senza chiederci permesso (o meglio, estorcendolo con quei contratti online che firmiamo senza leggere... e che è inutile leggere). Oggi tutti questi big data sono nelle mani

dei "capitalisti della sorveglianza", senza alcun controllo. Nella prima fase gli algoritmi hanno imparato a prevedere le nostre scelte, con margini di incertezza sempre minori. Ora si stanno attrezzando per orientare le nostre decisioni.

Le società di assicurazione vorrebbero da sempre ottenere un profilo preciso del cliente e del suo comportamento, per ridurre i margini di rischio ed eventualmente spingerlo entro determinati parametri comportamentali. Per farlo è necessario monitorare le azioni dell'automobilista, che però diffida di questa intrusione nella privacy e non si fida dell'azienda che vuole controllarlo. Se "il denaro non è abbastanza convincente, si consiglia agli assicuratori di presentare il monitoraggio del comportamento come 'divertente', 'interattivo', 'competitivo' e 'gratificante' (...) Questo approccio, noto come *gamification*, incoraggia i conducenti a partecipare a 'gare basate sulla performance' e a 'sfide fondate sugli incentivi'" (pp. 230-231). Meccanismi di condizionamento analoghi, che mirano a cambiare il comportamento degli utenti, si possono applicare alla sanità o all'istruzione.
Se il presupposto è l'ubiquità della sorveglianza, l'obiettivo, il vero potere, "è quello di *modificare* le azioni in tempo reale nel mondo reale. (...) Le analisi in tempo reale si traducono in azioni in tempo reale" (p. 309).

Anche in questo caso le strategie sono già affinate:
il *tuning*, che utilizza "indizi subliminali per dare forma impercettibilmente a un flusso di comportamenti" (ne sono esperti gli architetti delle case da gioco, per creare assuefazione negli scommettitori: ma anche internet e i social sono *addictive*);
lo *herding*, che lavora sul contesto che circonda la persona (perché l'invidia e i meccanismi imitativi, ovvero "l'influenza sociale", fanno parte del nostro bagaglio comportamentale) e punta a un "contagio emotivo";

il *condizionamento*, ben noto agli psicologi comportamentisti, che spinge gli animali (e dunque anche gli esseri umani) a selezionare i comportamenti di maggiore successo.
Il risultato è devastante: "Affermando di poter modificare le azioni umane in modo segreto e a scopo di lucro, il capitalismo della sorveglianza di fatto ci esilia dal nostro stesso comportamento, cambiando l'espressione del futuro 'io vorrò' a 'tu vorrai" (p. 325). Per Zuboff, stiamo perdendo la nostra libertà a favore del Grande Altro che rende gli individui oggetti. Non siamo stati vittime di un colpo di Stato, ma di un *coup de gens*: consumatori e cittadini sono schiacciati da una gigantesca asimmetria dell'informazione, nelle mani di poche aziende e di un potere politico più o meno occulto ma sicuramente antidemocratico.

I due internet secondo Edward Snowden

Anche i servizi segreti americani hanno costruito un internet parallelo, in grado di raccogliere valanghe di informazioni sui cittadini americani (e non solo), a loro insaputa (e senza informare gli organi democratici). Quando si accorse dell'esistenza di questo *deep State* – il programma PRISM con la *upstream collection*, ovvero la "raccolta a monte" dei dati dei cittadini – Edward Snowden era un nerd che lavorava per la National Security Agency, ovvero i servizi segreti USA. Restò sbalordito, sconvolto, indignato, come racconta nel suo autobiografico *Errore di sistema* (Longanesi, Milano, 2019, 350 pagine, 18,60 €).
"Immaginate di sedervi al computer per visitare un sito web. Aprite un browser, digitate un indirizzo e premete INVIO. La vostra azione equivale a una richiesta, e tale richiesta parte alla ricerca del server di destinazione. A un certo punto del suo viaggio verso il server, però, la vostra richiesta dovrà passare attraverso TURBULENCE, una delle armi più potenti dell'NSA". Ogni interazione in rete viene filtrata. La NSA, se ritiene che ci sia qualcosa di sospetto, installa sul vostro computer un malware da usare contro di voi: "In meno di 686 millisecondi ottenete tutti i contenuti che volevate, assieme a tutta la sorveglianza che non volevate" (pp. 225-226), senza passare dal giudice. La Intelligence Community degli Stati Uniti aveva "hackerato la Costituzione", alla quale Snowden voleva restare fedele. Si trovò lacerato da un dilemma tragico: tacere, per garantirsi una carriera e una vita tranquilla ma portandosi dentro quest'ombra, oppure...
Scegliere di non lavorare più "per il governo" ma "per le persone" non fu una una decisione facile, per il rampollo di una dinastia di fedeli servitori dello Stato. Come Snowden sia riuscito a trafugare e rendere pubblici ai primi di agosto del 2013 migliaia di documenti segreti senza farsi arrestare e senza impazzire, diventando uno dei più celebri *whistleblowers* della storia, è meglio scoprirlo leggendo la sua emozionante epopea solitaria (e lo struggente diario della sua compagna Lindsay nei giorni cruciali).

Onniscienza, controllo, certezza

Nell'indifferenza pressoché generale si è generato un sistema feroce, mostruoso, occulto. Come sia stato possibile, ce lo spiegano Snowden e Zuboff. Le cause sono molteplici. Il rapporto costante tra i servizi segreti e le aziende, fin dalla nascita di internet, che in origine era un'infrastruttura militare (ARPANET). Un'ideologia neo-liberista e individualista, che ha ridotto le tutele di leggi e regolamenti, dando spazio all'iniziativa privata senza alcun contrappeso della società civile e dei lavoratori. La necessità di alcune grandi aziende di massimizzare i profitti e ripagare gli azionisti dopo la bolla del 2000. L'ossessione per la sicurezza dopo l'11 settembre 2001.
Contribuisce anche, spiega Zuboff, la visione utopica di alcuni signori della rete. Larry Brin e Sergei Page di Google, come Mark Zuckerberg di Facebook, sono convinti che i loro algoritmi renderanno il mondo migliore: offrono "soluzioni ai singoli individui sotto forma di connessioni sociali, accesso all'informazione, risparmio di tempo, e spesso con l'illusione di un sostegno", e offrono "soluzioni alle istituzioni sotto forma di onniscienza, controllo e certezza". A differenza degli utopisti del passato, che erano filosofi squattrinati, questi profeti 2.0 dispongono di enormi risorse finanziarie per imporci le loro visioni.
Il loro intento, avverte Zuboff, "non è quello di porre rimedio all'instabilità – la corrosione della fiducia sociale, la rottura dei legami di reciprocità, le conseguenze pericolose dell'ineguaglianza, i regimi basati sull'esclusione – ma lo sfruttamento delle vulnerabilità prodotte da tali condizioni" (p. 400). Il "*cloud* che lavora in armonia con i sensori intelligenti" dell'IoT sarà in grado di anticipare e prevenire le deviazioni dalla norma "prima che possano accadere", ha annunciato nel 2017 Satya Nadella, amministratore delegato di Microsoft. Come ha avvertito Evgeny Morozov, diventa possibile prevenire (o reprimere) il dissenso ancora prima che si manifesti, e addirittura prima che gli interessati siano consapevoli di essere fuori dalla norma (*Internet non salverà il mondo*, traduzione di Gianni Pannofino, Mondadori, Milano, 2014, 454 pagine, 19 €).

Negli Stati Uniti, a guidare la danza sono le grandi aziende, alleate con l'apparato statale. La Comunità Europea tenta di frenare questa ingerenza con i suoi regolamenti sui monopoli, sul copyright e sulla privacy (GDPR). In Cina, è lo Stato (ovvero il Partito Comunista) a governare il meccanismo.

Sesame Credit, il sistema di "calcolo dei crediti personali" di Ant Financial (Ali Baba), valuta il regolare pagamento di crediti e bollette, ma anche "gli acquisti (videogame anziché libri per bambini), livello d'istruzione, quantità e 'qualità' degli amici". Usando questi dati, l'algoritmo decide chi può acquistare un biglietto d'aereo o per un treno ad alta velocità e chi deve invece viaggiare su un Regionale, chi può iscriversi al Partito e chi non può comprare una casa (Zuboff, pp. 407-408). Gli utenti di Sesame Credit hanno subito iniziato a ripagare i loro debiti alla banca.

Di recente i big data sono stati integrati con la geolocalizzazione (la strada l'ha tracciata un esperimento di massa come *Pokemon Go!*) e il riconoscimento facciale: il risultato è il *social credit* personale, un incubo che sembra una puntata di *Black Mirror*, come racconta il documentario *Social*

Credit: China's Digital Dystopia In The Making (https://www.youtube.com/watch?v=evBzPwCdeHI). Il social credit si rivela utilissimo per zittire ogni dissenso. Anche per questo la lotta degli studenti di Hong Kong è doppiamente eroica.

Una sovversione che viene dall'alto

Zuboff si chiede come possiamo resistere alla "macchina alveare nella quale rinunciamo alla libertà in cambio di una conoscenza perfetta che qualcun altro amministra per il proprio profitto" (p. 459). È un problema politico: "*Chi sa? Chi decide? Chi decide chi decide?*" È anche una questione di benessere psichico. "La scomparsa della società tradizionale e l'evoluzione della complessità sociale hanno accelerato il processo di individualizzazione". Dunque "la connessione digitale è divenuta un mezzo di partecipazione sociale necessario", ma dominato e strumentalizzato dal capitalismo della sorveglianza. Costruiamo la nostra identità sulla base del confronto sociale: ma più il bisogno degli altri viene soddisfatto (con il mix di esibizionismo e narcisismo tipico degli *influencer*), meno diventiamo capaci di costruire il nostro sé. Viviamo la *fear of missing out* (la "paura di perdersi qualcosa") e cadiamo preda dell'invidia.
Secondo una ricerca di Holly B. Shakya e Nicholas A. Christakis pubblicata nel 2017 sull'"American Journal of Epidemiology", mettere un like ai contenuti degli altri e cliccare sui loro link "sono azioni sempre collegate a problemi di benessere, mentre il numero degli status è collegato a una minor salute mentale [...] Una deviazione standard di 1 nel numero di like, [...] link cliccati [...] o aggiornamenti degli status viene associata a una diminuzione che va dal 5 all'8 per cento nelle condizioni di salute mentale riportate dal soggetto" (p. 480). Inutile precisare che questi dati forniscono al "testo ombra" valanghe di informazioni sullo stato personale dell'utente. La nostra interiorità, le nostre emozioni, sono diventate trasparenti, conoscibili e dunque manipolabili.
Tutto questo sta moltiplicando i profitti dei protagonisti del capitalismo della sorveglianza: i cinque big della rete (Amazon, Apple, Facebook, Google e Microsoft), ma anche i provider come Verizon, AT&T e Comcast, e poi le catene della distribuzione come Walmart, le grandi banche e assicurazioni, le piattaforme come AirBnB o eBay...

"La pressione del gruppo e la certezza computazionale sostituiscono politica e democrazia, annullando la percezione della realtà e la funzione sociale delle vite degli individui" (p. 31).
Come uscire da questo ossessivo e vorace *panopticon*? Come evitare di sprofondare in un nuovo totalitarismo? Come salvare una zona di intimità di fronte all'invadenza dei dispositivi? Come difendersi dalla violenza "oggettivante" degli algoritmi? Come ridurre gli errori di sistema, visto che – per esempio – quasi tutti i programmatori sono maschi bianchi con un alto livello di reddito e di istruzione? C'è un paradosso. Gli algoritmi usano il passato per predire il futuro e dunque perpetuano e amplificano i pregiudizi razzisti e maschilisti: questa gigantesca macchina per prevedere e realizzare il più radioso avvenire è per sua natura reazionaria, come ha dimostrato Cathy O'Neil (*Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, traduzione di Daria Cavallini, Bompiani, Milano, 2017, 368 pagine, 18 €).
Di fronte all'opacità e alla segretezza che accompagna questa rivoluzione, che ci vuole ignari come le cavie degli esperimenti degli etologi, il primo passo è la consapevolezza e l'acquisizione di uno spirito critico. Il secondo gesto è autodifensivo e ironico: possiamo "trasformare l'atto di nascondersi in una scienza e un'arte" (Zuboff, p. 504). Ma naturalmente per difenderci dalla "sovversione che viene dall'alto" servono azioni politiche e strumenti legislativi, e soprattutto una ampia mobilitazione democratica. È questa la sfida che ci lancia il capitalismo della sorveglianza. Non sarà una battaglia facile.

Ecco, sei arrivato fino in fondo a questo lungo post e dunque sei un'anomalia.
Per capire chi sei, mi basta guardarti in faccia e guardare le tue scarpe.
Lo stesso vale per te.
Adesso possiamo cominciare a parlare.