Lezione 2
Cenni storici

Sviluppo di software sicuro (9 CFU), LM Informatica, A. A. 2021/2022
Dipartimento di Scienze Fisiche, Informatiche e Matematiche
Università di Modena e Reggio Emilia
http://weblab.ing.unimore.it/people/andreolini/didattica/sviluppo-software-sicuro

Quote of the day

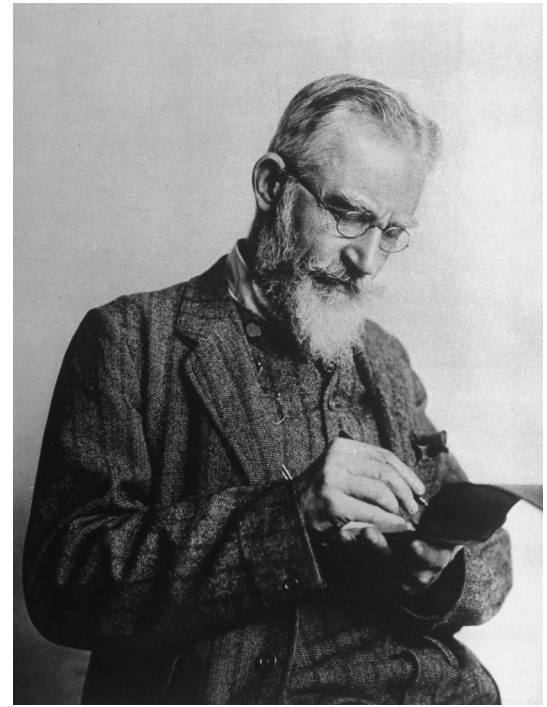
(Meditate, gente, meditate...)

“If history repeats itself, and the unexpected always happens, how incapable must Man be of learning from experience.”

George Bernard Shaw (1856 – 1950)

Scrittore, drammaturgo, linguista, critico musicale

Autore de “Il Pigmalione”



Sir John Ambrose Fleming (1849-1945)

(The electrical engineer and physicist)

Inventore, ingegnere, radiotecnico, elettrotecnico.

Inventore del diodo e della valvola termoionica.

Consulente (fra le altre) della Marconi Wireless Telegraph Company.

John Nevil Maskelyne (1839-1917)

(The magician)

Mago. Inventore del bagno pubblico "a gettone".

Fondatore del "Comitato Occulto" (antesignano dell'odierno CICAP).

1903: Maskelyne rovina una dimostrazione pubblica del telegrafo "sicuro" senza fili (svolta da Fleming).

Riesce ad inviare insulti in codice Morse...

Enigma (1926)

(The encryption/decryption machine)

Macchina elettro-meccanica usata per cifrare e decifrare messaggi.

Usata dalla Wehrmacht durante la Seconda Guerra Mondiale.

Considerata indecifrabile per lungo tempo.

Arthur Scherbius (1878-1929)

(L'inventore di Enigma)

Ingegnere tedesco.

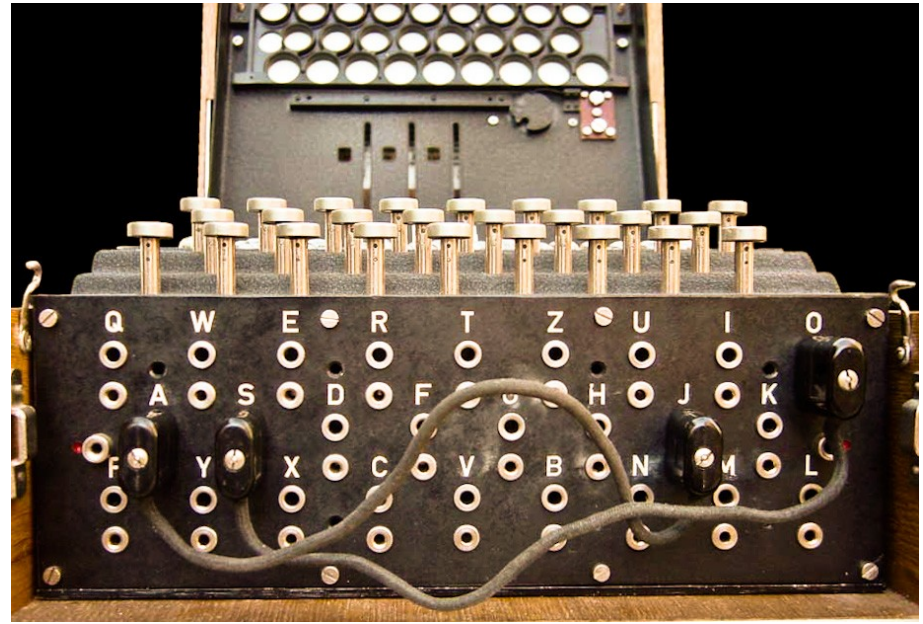
1918: brevetta Enigma (macchina cifrante basata su rotori).

1926: la Marina Militare tedesca adotta una variante di Enigma per le sue comunicazioni cifrate.

L'Enigma militare

(L'inventore di Enigma)

Uso di un pannello di controllo aggiuntivo (detto "plugboard") per offuscare ulteriormente il processo di cifratura.



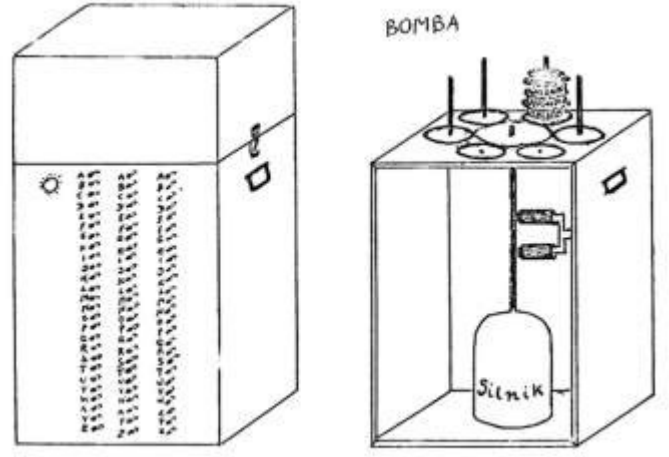
Bomba kryptologiczna (1938)

(Macchina in grado di decifrare la prima versione di Enigma)

1932: studio teorico condotto da polacchi "rompe" l'algoritmo di Enigma.

Inizia il progetto di una macchina "calcolatrice" in grado di rompere rapidamente il codice segreto criptato da Enigma.

→ "rapidamente" poiché i codici di Enigma venivano cambiati ogni giorno.



Outside and interior of Polish "bomba", drawing by Rejewski, 1978

Bomba kryptologiczna (1938)

(Macchina in grado di decifrare la prima versione di Enigma)

1932-1937: costruzione ed evoluzione di una macchina calcolatrice (“bomba crittologica”) in grado di

- ricostruire velocemente la posizione dei rotori di Enigma
- decifrare i messaggi prodotti da Enigma

1938: i polacchi hanno una macchina calcolatrice in grado di decifrare rapidamente il codice Enigma.

Marian Rejewski (1905-1980)

(L'autore dello studio teorico del 1932; il coautore di "Bomba")

Matematico e crittografo.

1929: durante gli studi universitari a Poznam, segue un corso segreto di crittografia presso lo Stato Maggiore polacco.

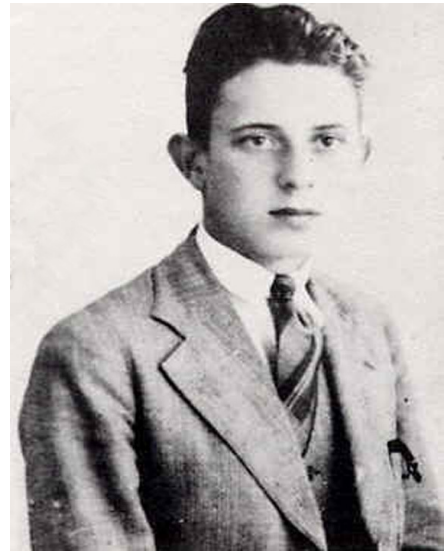
1932: viene assunto dall'Ufficio Crittografico dell'esercito polacco.

Dopo poche settimane individua e rompe il primo algoritmo di Enigma.

I coautori dello studio del 1932

(Henryk Zygalski e Jerzy Rozycki)

Henryk Zygalski
(1908-1978)



Jerzy Rozycki
(1909-1942)

Evoluzione di Enigma (1938-1939)

(Macchina in grado di decifrare la seconda versione di Enigma)

1938-1939: i nazisti cambiano la struttura di Enigma.

- Quattro rotori al posto di tre
- Una plugboard aggiuntiva che funge da rotore

→ La bomba crittologica non è più in grado di decifrare i messaggi in maniera rapida.

Un incontro importante (1939-1942)

(I polacchi condividono le loro conoscenze con inglesi e francesi)

Luglio 1939: cinque settimane dopo l'invasione della Polonia da parte dei nazisti, Rejewski ed i suoi colleghi presentano i loro studi ai colleghi francesi ed inglesi.

1939-1942: i polacchi, costretti all'esilio in Francia, collaborano con i loro colleghi francesi.

Il progetto di Bombe (1939)

(Macchina in grado di decifrare la seconda versione di Enigma)

1939: a Bletchley Park viene completato il progetto di "Bombe", una nuova macchina calcolatrice con l'obiettivo di rompere nuovamente Enigma.

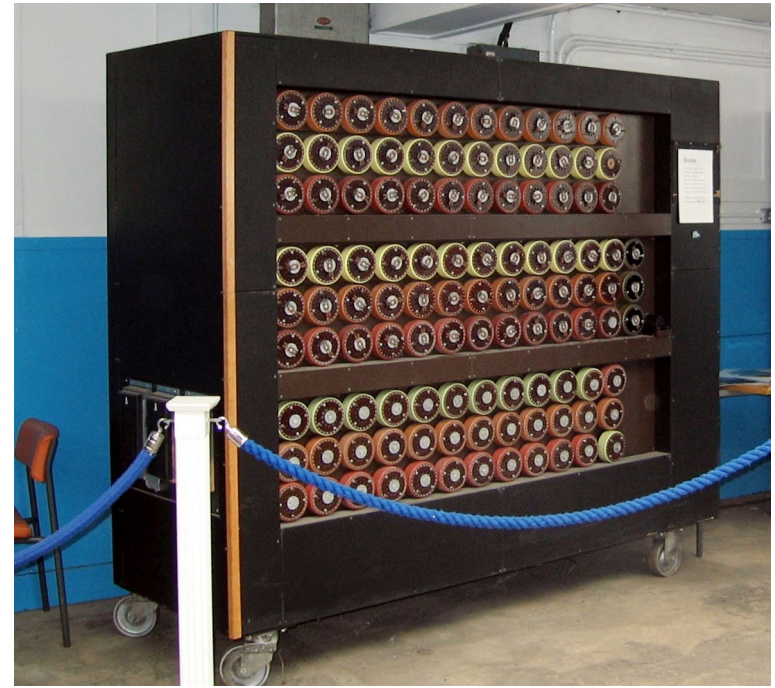
L'evoluzione di Bombe (1940-1944)

(Macchina in grado di decifrare la seconda versione di Enigma)

1940: primo prototipo in grado di rompere Enigma classico.

1941: scoperta di Enigma a quattro rotori (grazie ad errori commessi dai nazisti).

- Invio di messaggi con il quarto rotore in posizione sbagliata
- Reinvio degli stessi messaggi con il quarto rotore in posizione corretta



L'evoluzione di Bombe (1940-1944)

(Macchina in grado di decifrare la seconda versione di Enigma)

1942: rottura del cifrario Enigma a quattro rotori.

Uso di un metodo di attacco alternativo: **Known Plaintext Attack**.

- Si assume noto il testo in chiaro corrispondente ad una porzione di testo cifrato.
- Si prova a rompere il cifrario con questa informazione aggiuntiva.

- → Approccio molto più efficiente della bomba crittologica polacca, che operava a forza bruta.

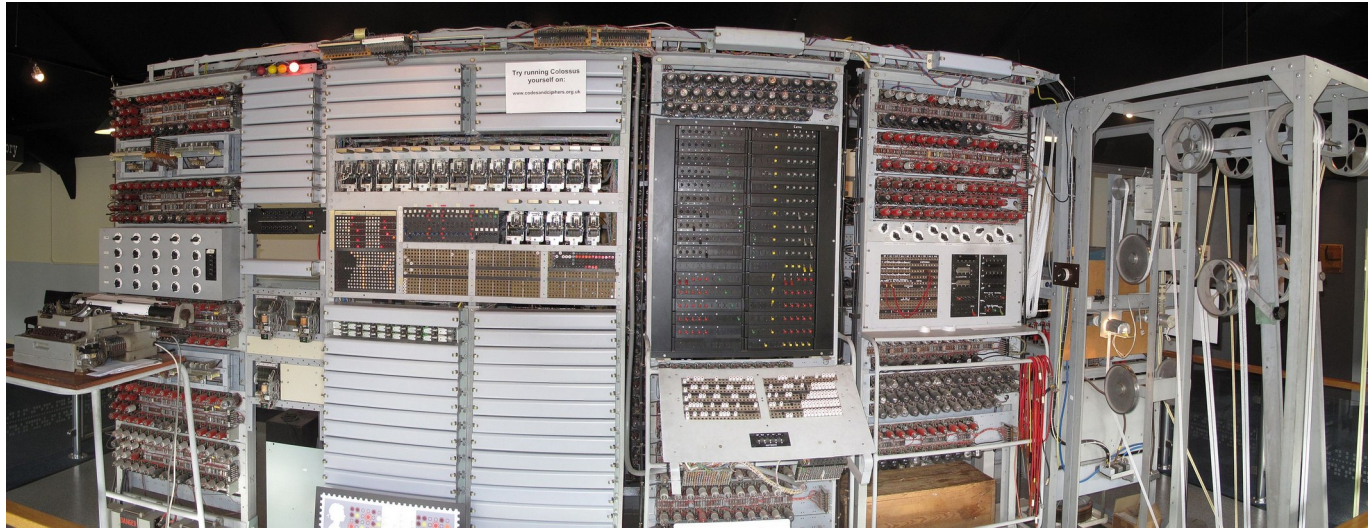
Colossus (1944)

(L'evoluzione di Enigma)

Primo calcolatore digitale britannico. Evoluzione di Bombe.
Usato inizialmente per rompere il cifrario di Lorenz.

- Cifrario "classificato" dei nazisti

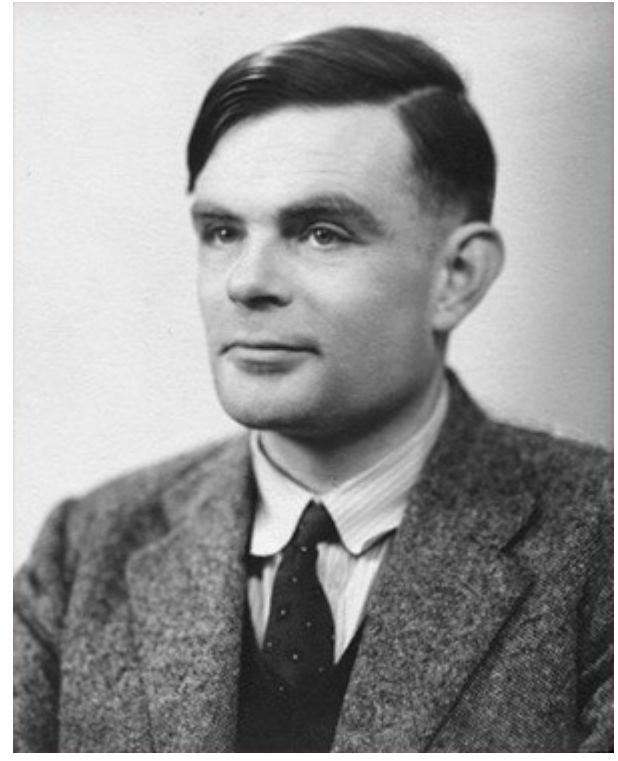
Programmabile mediante switch. Output su telescrivente.
Antesignano dei moderni calcolatori.



Alan Turing (1912-1954)

(Rompe Enigma per la seconda volta, fra le tante altre cose...)

Matematico. Criptoanalista.
Pioniere dell'Informatica moderna.
1939: costruisce "Bombe". Bombe è inizializzata con messaggi cifrati il cui contenuto in chiaro è noto.
1944: costruisce "Colossus", prototipo del primo calcolatore moderno.



Gordon Welchman (1906-1985)

(Il "capo" di Turing)

Matematico. Criptoanalista.
Professore Universitario.
Capo dell'unità di cifratura nell'Hut 8 (dove lavora Turing).

Harold "Doc" Keen (1894-1973)

(Il costruttore di Bombe)

Ingegnere.
Progetta e costruisce Bombe.

René Carmille (1886-1945)

(Precursore degli "ethical hacker")

Revisore dei conti militare, esperto di schede perforate. "Agente doppio" durante la Resistenza francese.

"Sabotatore etico" del meccanismo di censimento automatico degli ebrei operato dai nazisti nella Francia occupata.

- Alterazione delle schede perforate.
- Riprogrammazione delle macchine perforanti.

MIT Tech Model Railroad Club

(The wellspring of hacker culture)

Circolo di modellismo ferroviario del MIT (1946-).

Membri: professori, studenti, appassionati di modellismo.

Passione condivisa: capire la natura delle cose e saperla controllare in modo creativo.

→ “Hacking”.

“Uncle” John McCarthy (1927-2011)

(Pioniere dell’AI, creatore del LISP)

Matematico. Pioniere dell’Informatica moderna. Inventore del termine “Intelligenza Artificiale”.
Inventore del linguaggio LISP.
Progettista del linguaggio Algol.
Precursore del time-sharing.
Membro del MIT Tech Railroad Club.

Jack Dennis (1931-)

(Padre di MULTICS, nonno di UNIX, bisnonno di GNU/Linux)

1964: Coinventore del SO MULTICS (con Corbato e Fano).

"Padre" di UNIX (a sua volta "padre" di GNU/Linux).

Membro del MIT Tech Railroad Club.

Jack Dennis (1931-) | Fernando J. Corbato (1926-) | Roberto Mario Fano (1917-2016)

Peter Deutsch (1946-)

(Padre di Smalltalk, nonno di Ruby)

Informatico.

1963: autore del LISP 1.5 per PDP-1.

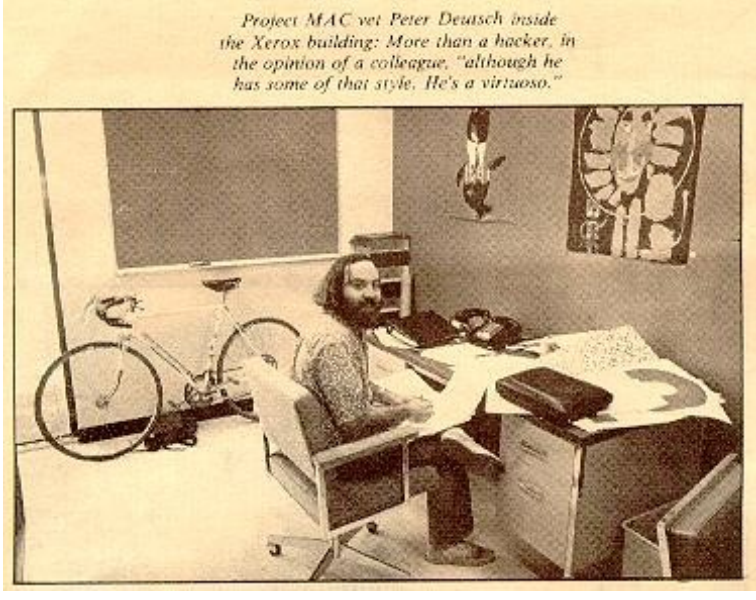
1972: creatore del primo compilatore JIT (Smalltalk).

Smalltalk → "nonno" di Ruby.

1988: creatore di Ghostscript.

Autore di diversi RFC IETF.

Membro del MIT Tech Railroad Club.



Project MAC vet Peter Deutsch inside the Xerox building: More than a hacker, in the opinion of a colleague, "although he has some of that style. He's a virtuoso."

Alan Kotok (1941-2006)

(The first true hacker)

Informatico.

1960: coautore del primo videogioco (Spacewar!) con Steve Russell.

1994: fonda il W3C.

Membro del MIT Tech Railroad Club.

Presenta ai suoi colleghi il computer TX-0, con cui ci si divertiva la notte...

→ Spostamento dai trenini ai computer...

Alan Kotok (1941-2006) Steve Russell (1937-)

TX-0

(Il computer che ispirerà i PDP)

1955: computer progettato al MIT. Basato su transistor.

- Processore a 18 bit.
- Spazio indirizzi a 16 bit.
- 4KB di memoria a nuclei di ferrite.

Il primo computer usato dagli "hacker" del MIT Tech Railroad Club.

1961: DEC semplifica il progetto del TX-0 e produce il PDP-1.

Richard Greenblatt (1944-)

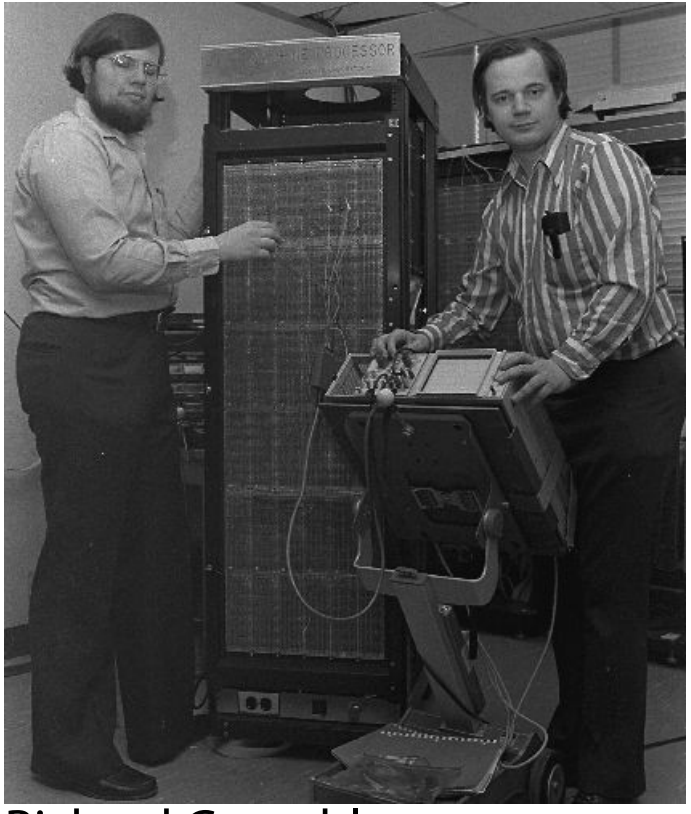
(The first computer hacker)

Programmatore.

1962: scrive un compilatore Fortran per il PDP-1, in modo da poter eseguire un programma di controllo dei binari scritto per l'IBM 7090.

1969: scrive Incompatible Time Sharing System, il SO usato al MIT CSAIL, dove ha fondato la prima comunità hacker informatica.

Membro del MIT Tech Railroad Club.



Richard Greenblatt (1941-)

Josef Carl Engressia, Jr. (1949-2007)

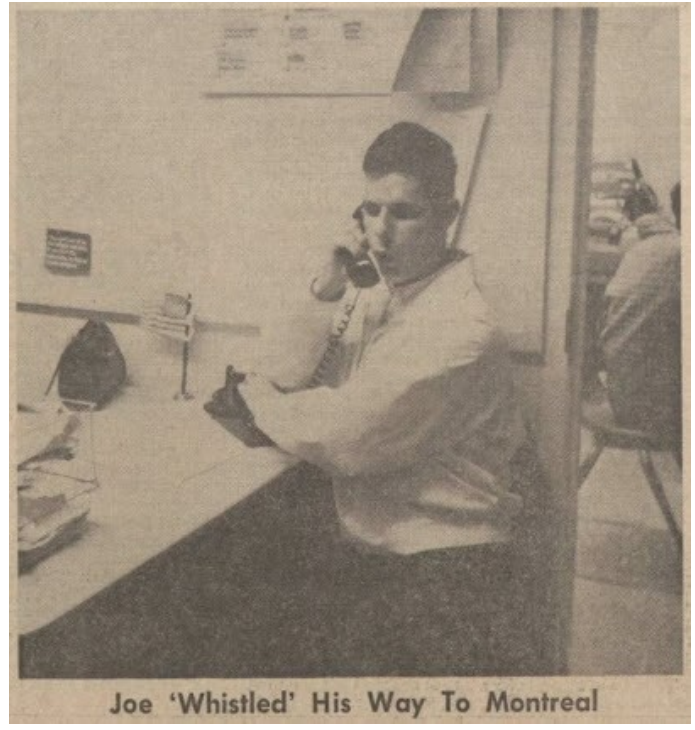
(Joybubbles, possibly the first modern phone phreaker)

Laureato in filosofia.

Non vedente, dotato del cosiddetto "orecchio assoluto" (capacità di riprodurre una nota esattamente).

1956: scopre che, riproducendo un suono alla frequenza di 2600Hz, è possibile attivare gli switch telefonici AT&T, telefonando gratis.

1971: viene infine arrestato.



Joe 'Whistled' His Way To Montreal

Il primo "hack" malizioso

(War dialing sul PDP-1 di Harvard)

1963: il giornale degli studenti del MIT (The Tech) riferisce di una intrusione nel PDP-1 di Harvard, riprogrammato per scandire i numeri di telefono alla ricerca di altri calcolatori.

→ War dialing.

Lo scherzo porta ad una bolletta telefonica astronomica per Harvard.

Divulgazione della prima vulnerabilità

(Operata nel 1965 da David Matthews per CTSS di IBM 7094)

1965: David Matthews del MIT scopre un difetto nel SO CTSS (Compatible Time Sharing System) su un IBM 7094.

Se due utenti aprono l'editor simultaneamente, i file delle password e del "message of the day" si scambiano (!?!).

→ Ogni utente che si autentica vede tutte le password utente.

John Draper (1943-)

(Captain Crunch, phone phreaker extraordinaire)

Programmatore. Phone phreak.

1971: Draper scopre che un fischietto giocattolo contenuto nelle scatole di cereali "Captain Crunch" riproduce la stessa frequenza a 2600Hz usata da Joybubbles per telefonare a sbafo.

Crea la "Blue Box", dispositivo per il phone phreaking.

Viene in seguito arrestato.

John Draper (1943-)

Captain crunch, il fischietto, la blue box

(Gli altri protagonisti della vicenda Draper)

Captain Crunch
(1971)

Il fischietto

Steve “The Woz” Wozniak (1950-) con la Blue Box di John Draper.

Kevin David Mitnick (1963-)

(Il primo social engineer)

Consulente di sicurezza, cracker.

Pioniere di due tecniche di attacco.

- Social Engineering: manipolazione psicologica delle persone atta a rivelare dati sensibili.
- Dumpster diving: ricerca di dati sensibili nei rifiuti.

1979: viola Ark (DEC) e ruba il software della Digital. Viene arrestato nel 1988.

1982: viola la rete militare del NORAD.

1992: rilasciato, viola il sistema voice mail di Bell. Si dà alla latitanza.

1995: viene nuovamente arrestato.

La breccia della National CSS

(Cosa può arrivare a fare un dipendente annoiato...)

1980: l'FBI investiga una breccia di sicurezza avvenuta presso la National CSS.

- Fornitrice di servizi time-sharing.
- Antesignana del cloud computing.

Un tecnico annoiato viola la "master password" del sistema usando un password cracker in sua dotazione.

FBI e NCSS imparano a proprie spese che:

- possono esistere attaccanti "interni";
- giovani talenti possono attaccare un sistema per il semplice gusto di farlo.

White/Black hat, interni/esterni

(Una prima tassonomia degli attaccanti)

1981: un articolo sul New York Times dettaglia i risultati dell'indagine.

L'articolo parla di attaccanti interni ed esterni, nonché di **white hat** e **black hat**.

White hat: esplora i limiti di un sistema senza avere fini di lucro (pur violando la legge).

Black hat: esplora i limiti di un sistema per fini di lucro.

Elk Cloner

(Il primo virus a larga diffusione)

1981: Richard "Rich" Skrenta crea "Elk Cloner", un software per Apple II che, se eseguito, svolge le seguenti operazioni.

- Monitora le operazioni di I/O.
- Se individua un floppy non contagiato, si riproduce nel suo settore di boot.

Ad ogni 50mo avvio del floppy infetto, il virus stampa un messaggio e si riproduce.

1982: grazie all'attività di pirateria dei videogiochi, il virus si diffonde su scala nazionale!

Rich Skrenta
(1967-)

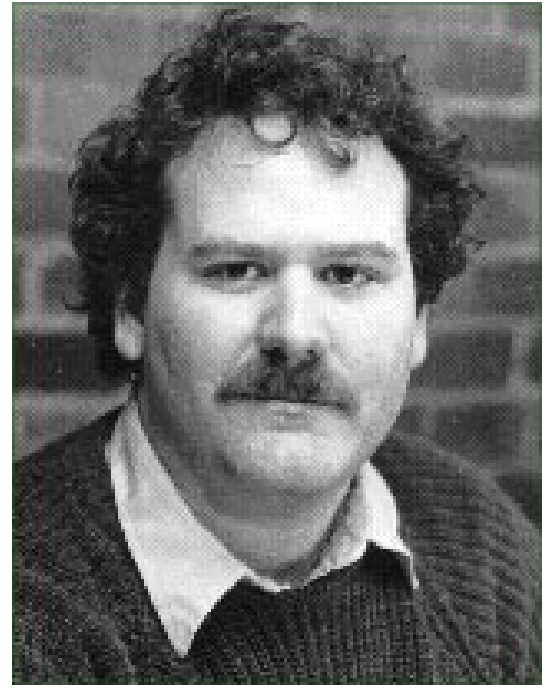
Uso del termine "Computer virus"

(Introdotto ufficialmente nel 1984 da Fred Cohen)

Il termine "Computer Virus" non viene subito adottato per descrivere il comportamento di Elk Cloner.

1984: Fred Cohen (Univ. South California) introduce il termine nel suo articolo scientifico "Computer Viruses – Theory and Experiments".

1987: Fred Cohen dimostra che il problema della rilevazione dei virus è indecidibile.



Chaos Computer Club

(Il primo collettivo moderno di "hacker")

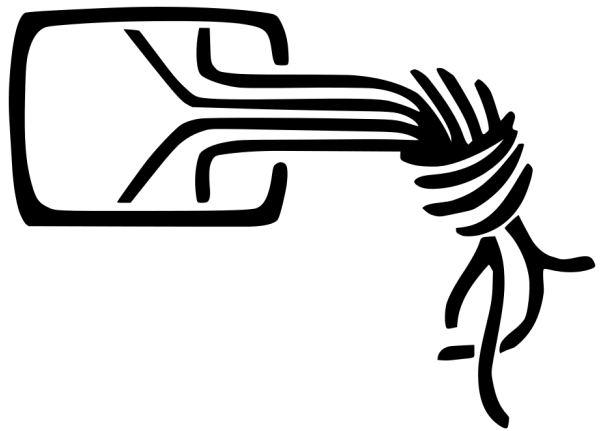
1981: nasce in Germania il Chaos Computer Club.

- Il più antico (e grande) collettivo di "hacker" attivo ad oggi.

Motivazioni:

- libertà di informazione.
- diritto umano alla comunicazione.
- "hacker ethic", attivismo.

Gestisce il Chaos Communication Congress annuale (la più grande riunione di hacker in Europa).



Ian Murphy (?-)

(AKA "Captain Zap")

Consulente di sicurezza.

Un tempo, criminale informatico.

1981: Ian Murphy irrompe nei server dell'AT&T e modifica i contatori delle tariffe.

Nello stesso anno viene arrestato, processato e condannato.

Primo "hacker" condannato per un crimine informatico.

Kenneth Lane "ken" Thompson (1943-)

(Autore di UNIX; vincitore del Turing Award nel 1983)

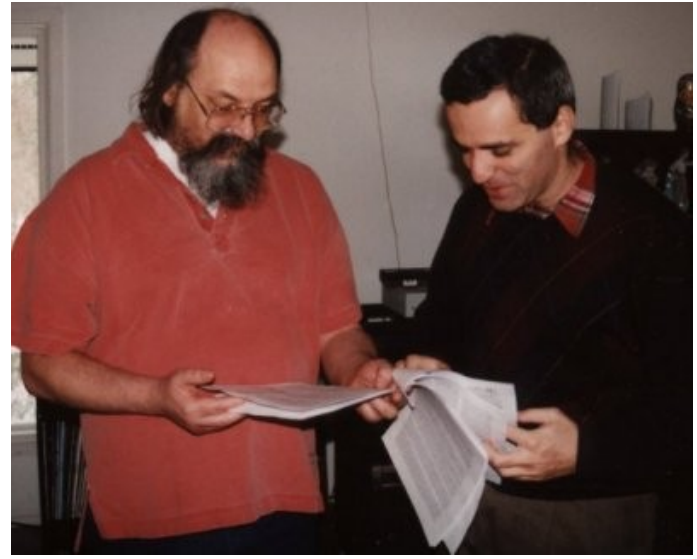
Informatico.

1969: coautore di UNIX (con Dennis Ritchie).

1983: vince il premio Turing (Nobel dell'Informatica) insieme a Dennis Ritchie.

Lectio Magistralis del premio Turing: "Reflections on trusting trust".

Cavallo di Troia "invisibile" inserito nel compilatore UNIX.



Ken Thompson (1943-)

Legion of Doom

(Il collettivo di hacker più bravo degli anni '80)

1984: "Lex Luthor" fonda la "Legion of Doom" (il collettivo di hacker più bravo nel periodo 1984-1991).

1985: uno dei membri di LoD, "Erik BloodAxe" (al secolo, Chris Goggans) fonderà la rivista online "Phrack".

Hacking "white" e "black", phreaking, anarchia, controcultura.

Phrack è, ad oggi, la rivista online più prestigiosa in ambito di sicurezza.

Molto più delle riviste accademiche...

Chris Goggans
AKA
Erik Bloodaxe
(1969-)

Cult of the Dead Cow

(Il collettivo di hacker più bravo degli anni '80)

1984: nasce in Texas il collettivo hacker "Cult of the Dead Cow" (cDc).

- Connessione tramite BBS.
- White hat, black hat, phreaking, anarchia.

Il cDc inventa l'alfabeto "elite".

- 31337 → "eleet" (elite hacker)

1994: hacker "Omega" di cDc conia il termine "hacktivism".

- Uso sovversivo di (reti di) computer per promuovere una agenda politica.

1998: hacker "Sir Dystic" crea "Back Orifice", primo esempio di **Remote Administration Tool** (**RAT**).

Christmas Tree EXEC

(Il primo programma che si riproduce automaticamente)

1987: uno studente alla Clausthal University of Technology scrive “Christmas Tree EXEC”.

Stampa a video un albero di Natale.

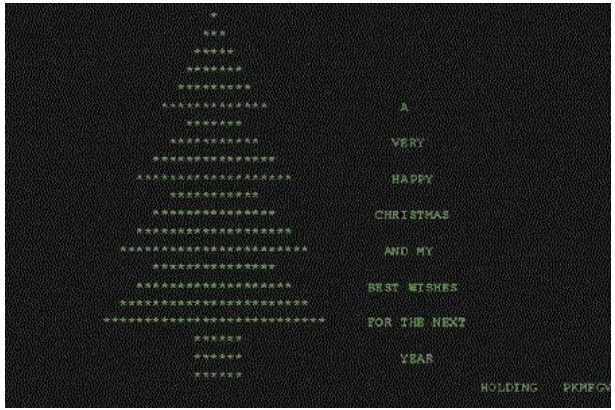
Si invia a tutti i contatti di posta elettronica e si esegue.

Crea grossi disservizi nelle seguenti reti:

European Academic Research Network;

BITNET;

IBM VNET.



I primi anti-virus

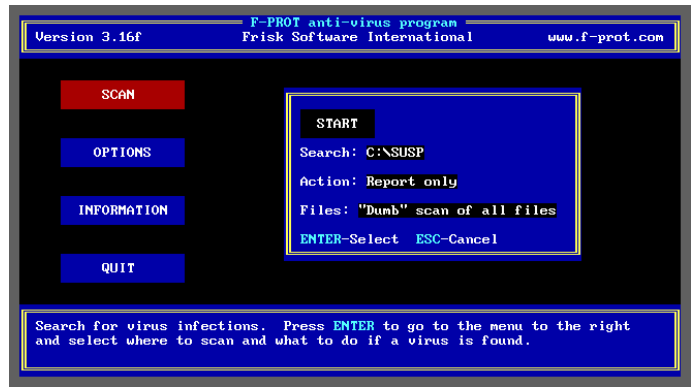
(Fine anni '80 – inizio anni '90)

1987: Bernd Fix propone la prima procedura di rimozione di un virus.

1987: Andreas Luening e Kai Fugge fondano G Data Software, rilasciando il primo antivirus per l'Atari ST.

1991: viene rilasciato F-PROT, il prototipo di antivirus moderno basato su due tecniche di rilevazione:

- firme (signature) rilevazione "a riposo";
- euristiche per la rilevazione "in esecuzione".



F-PROT (1991)

Computer Worm

(Più raffinato di un Computer Virus)

Il comportamento ora menzionato è più raffinato di quello esibito da un virus.

Il virus non si trasmette automaticamente (infetta solamente dischi).

Christmas Tree EXEC si riproduce automaticamente su altre macchine, sfruttando una connessione di rete.

A tale comportamento è stato dato il nome di **Computer Worm** (cfr. slide seguente).

Robert Morris (1965-)

(Autore del famigerato worm)

Professore universitario.

1988: in qualità di dottorando alla Cornell University, ha accesso ad ARPANET. Scrive un programma che si riproduce su ARPANET in maniera discreta.

Chiama **worm** (verme) il programma, perché "striscia tra le macchine come un verme".

Funzionamento del worm

(A grandi linee)

Per riprodursi, worm usa falle presenti in software UNIX popolari, quali sendmail, finger, rsh.

Una volta trasferito su una nuova macchina, worm controlla se è già installato.

Se non lo è, si installa.

Se lo è, si installa comunque (in media, una volta su sette macchine).

L'impatto del worm

(Mette fuori uso 1/10 di ARPANET)

2/11/1988 ore 18: il worm è lanciato da uno dei computer del MIT (per camuffare la vera origine – Cornell).

Il worm si propaga velocemente e si reinstalla centinaia di volte sulle stesse macchine, portandole al collasso.

Circa il 10% delle macchine connesse ad ARPANET (6000 computer) va fuori uso.

Danno stimato: 98 milioni di dollari.

Le conseguenze (legali e tecniche)

(Morris è arrestato; gli USA creano il CERT)

Conseguenze legali. Robert Morris è condannato a tre anni di libertà condizionata, 400 ore di servizi socialmente utili e 10050 dollari di multa.

Conseguenze tecniche. Il DARPA crea presso la Carnegie Mellon University il primo Computer Emergency Response Team (CERT).

- Team di esperti di rete e di sicurezza preposto all'analisi degli incidenti ed al ripristino dell'operatività di rete.

CERT

Software Engineering Institute
Carnegie Mellon University

AIDS trojan horse

(Il primo ransomware della storia)

1989: il trojan "AIDS" è il primo a chiedere un riscatto per il ripristino del PC infetto (**ransomware**).

L'operazione "Sundevil"

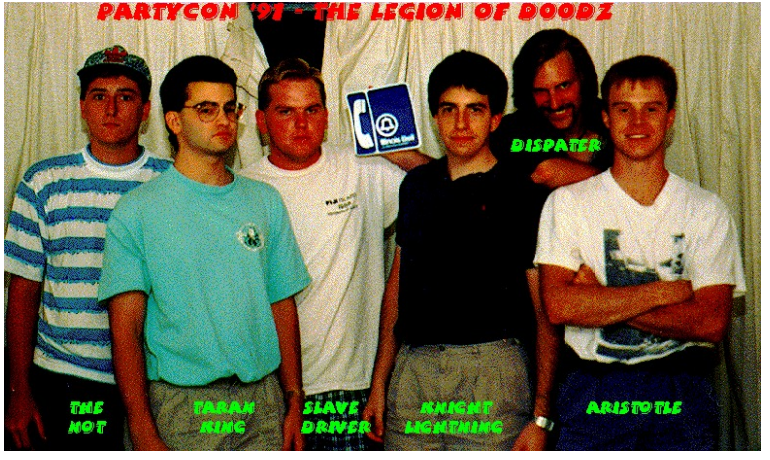
(Porta alla nascita della Electronic Frontier Foundation)

1990: l'intelligence americana arresta i membri principali delle BBS della Legion Of Doom.

Uno degli arrestati (Craig Neidorf, AKA "Knight Lightning") è uno dei fondatori della rivista "Phrack".

Luglio 1990: in risposta al blitz, viene fondata la Electronic Frontier Foundation (**EFF**).

- Associazione no-profit.
- Monitoraggio di abusi aziendali e/o governativi su hacker (agli inizi) e sulla popolazione (in seguito).



Craig Neidorf
(1969-)

Il virus 1260

(Primo virus polimorfico)

1992: lo scrittore di virus “Dark Avenger” scrive **1260**, il primo virus polimorfico.

Virus polimorfico: il codice che lo esegue cambia lievemente ad ogni esecuzione.

Il virus si riproduce cifrandosi ogni volta con una chiave diversa.

Un decrittatore variabile è inserito in testa al virus cifrato.

→ È in grado di aggirare i normali controlli di un antivirus.

DEFCON

(La top conference in ambito di sicurezza)

1993: si tiene a Las Vegas la prima conferenza DEFCON.

Ad oggi, DEFCON è la conferenza più grande e più apprezzata in ambito di sicurezza.

Vlamidir Levin (1967-)

(Autore di una stangata da dieci milioni di dollari, finita molto male)

Matematico biochimico (o, forse, semplice amministratore di sistema).

1994: riesce ad accedere ai conti di tantissimi clienti di CitiBank (una banca americana) e li trasferisce su conti finlandesi ed israeliani.

Tre suoi complici sono arrestati nel tentativo di riscuotere i soldi.

1995: viene arrestato all'aeroporto di Londra.

1997: viene estradato negli USA.

1998: viene condannato a tre anni di carcere.

David L. Smith (1967-)

(Macro virus: si propaga su diversi SO attraverso applicazioni da ufficio)

26 marzo 1999: David L. Smith (un dipendente della municipalità di Aberdeen) rilascia il virus **Melissa**.

Melissa è un **macro virus**: è scritto in un linguaggio macro fornito con una applicazione da ufficio (ad es., Office).

→ È in grado di diffondersi su diversi ambienti operativi.

10 dicembre 1999: Smith è condannato a 10 anni di reclusione e ad una multa di 5000 dollari.

Dmitry Sklyarov (1974-)

(Condannato per aver violato la sicurezza dei prodotti Adobe)

Cittadino russo.

Dipendente della ditta ElcomSoft (specializzata in audit di sicurezza e recupero di password).

2001: viene invitato a DEFCON per presentare un lavoro dal titolo “eBook’s security – theory and practice”.

Viene arrestato per violazione del Digital Millennium Copyright Act (DCMA), su precisa accusa di Adobe.

Rilasciato su cauzione con l’aiuto della EFF.

Dicembre 2001: ritorno a Mosca.

Jan De Vit (1981-)

(Autore del virus "Anna Kournikova")

Programmatore.

2001: scrive il computer worm "Anna Kournikova".

Si diffonde tramite un allegato e-mail con una immagine "sexy" della tennista Anna Kournikova.

Se aperto, l'allegato esegue uno script Visual Basic che diffonde il worm ad ogni indirizzo nella rubrica della vittima.

Danni stimati (in mailbox lockdown): 166827 dollari.

Le conseguenze legali

(150 giorni di servizi sociali ed un'offerta di lavoro come tecnico informatico)

Non appena si rende conto della diffusione del worm, De Wit si costituisce alla polizia.

Nel frattempo l'FBI, con l'aiuto di David L. Smith (divenuto collaboratore sotto copertura), individua De Wit e lo segnala alle autorità olandesi.

De Wit è condannato a 150 ore di servizi sociali.

Il sindaco di Sneek gli offrirà un lavoro in qualità di tecnico informatico.

Rafael Núñez (1979-)

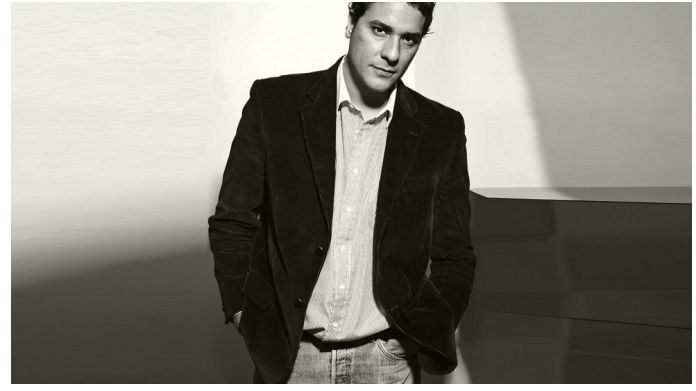
(AKA "RaFa", he 0wn3d the USAF)

Consulente di sicurezza.

Ex membro del collettivo World Of Hell.

2001: viola un computer della United States Air Force ed ottiene documenti confidenziali della NASA.

2005: viene arrestato all'ingresso negli USA. È stato successivamente estradato in Venezuela.



Jeanson James Ancheta (1985-)

(First known botnet op)

Barista. Aspirante soldato.

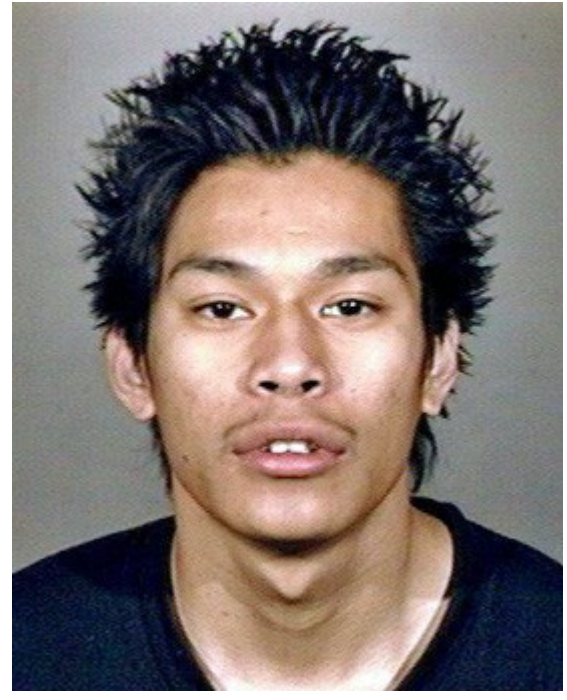
2004: modifica il worm **rxbot** per costruire una botnet.

Botnet: insieme di dispositivi connessi ad Internet (controllati solitamente da un operatore maligno) che svolgono operazioni illegali.

Invio SPAM, attacchi, esfiltrazione, …

Novembre 2005: è arrestato nell'ambito di una complessa operazione dell'FBI (operation Bot Roast).

2006: condannato a 60 mesi di carcere.



Estonia Cyber Attack

(Il primo attacco informatico ad un intero stato)

27 aprile 2007: l'Estonia inizia a subire una serie di **attacchi cibernetici** (**cyber attack**).

- Attacchi condotti tramite Internet.
- Tipologia: Distributed Denial of Service (DDoS).
- Obiettivi: infrastrutture critiche, banche, siti istituzionali, giornali, televisioni.

L'Estonia (un paese completamente informatizzato) è messa in ginocchio per un mese ed è sull'orlo del crack.

Attaccante: [redacted] .

Motivazioni: [redacted] .

Attacco all'OSD

(Il cuore del Pentagono)

2007: l'Ufficio del Segretario della Difesa (Office of Secretary of Defense, OSD), sito all'interno del Pentagono, è violato.

Vengono esfiltrati documenti top secret.

L'attacco utilizzato è uno **spear phishing**.

Spear phishing: attacco di phishing mirato ad uno specifico utente.

Phishing: tecnica di social engineering con cui si confonde una persona e la si induce a:

- fornire dati personali;
- installare software malizioso.

Conficker

(Long live MS08-67!)

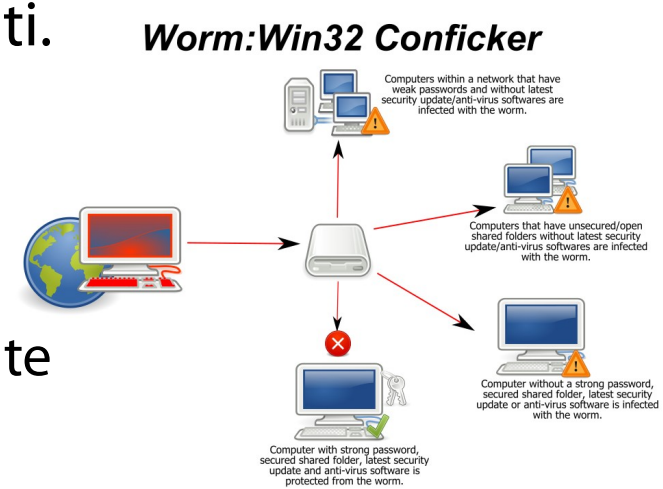
Conficker è uno dei worm più famigerati. Colpisce i SO Windows.

- Viola i SO sfruttandone difetti noti.
- Prova a recuperare le password utente.
- Si diffonde in rete locale tramite SMB.
- Forma una botnet semi-automaticamente tramite HTTP.

Novembre 2008: Conficker viene scoperto.

Ha infettato dai 9 ai 15 milioni di computer nel 2009 (prima di essere controllato).

- Molti di questi sono militari e governativi.



Operation Aurora

(Furto di proprietà intellettuale)

2010: Google rende pubblico di essere stato oggetto di una serie di attacchi cibernetici dal 2009.

- Obiettivo: furto di proprietà intellettuale.
- Attaccante: [redacted].
- Altre vittime: Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, Dow Chemical.

L'attacco è incredibilmente sofisticato, perdura nel tempo, coinvolge diversi obiettivi ed è molto difficile da sradicare.

→ **Advanced Persistent Threat** (**APT**).

Stuxnet

(Attacca infrastrutture industriali)

Stuxnet è un computer worm.

Attacca i sistemi di supervisione e controllo (SCADA) di Siemens ed i controllori logici programmabili industriali (PLC) in esecuzione su Windows.

Opera usando difetti non noti.

È capace di "nascondersi".

Vettore di inoculazione iniziale: chiavetta USB infetta.

2010: Stuxnet danneggia "casualmente" alcune centrali iraniane di produzione di uranio impoverito.

Attaccanti: [redacted].

Linkedin data leak

(6,5 millions passwords stolen)

5 giugno 2012: la rete sociale Linkedin viene violata. Circa 6,5 milioni di password degli utenti sono trafugate.

Attaccante: cyber criminali russi.

Gli utenti lanciano una class action da 5 milioni di dollari.

Ci si accorda per un risarcimento globale di 1.25 milioni di dollari.

Mt. Gox bitcoin exchange hack

(Went downhill afterwards)

2014: il servizio di compravendita di moneta virtuale (bitcoin exchange) più usato (Mt. Gox) viene violato.

Ben 460 milioni di dollari in valuta virtuale sono rubati dagli attaccanti.

Altri 27.4 milioni di dollari sono prelevati dai conti correnti.

Mt. Gox va in bancarotta poco tempo dopo.

Ashley Madison data leak

(Con conseguenze devastanti per le persone)

Luglio 2015: il sito di incontri online "Ashley Madison" è violato.

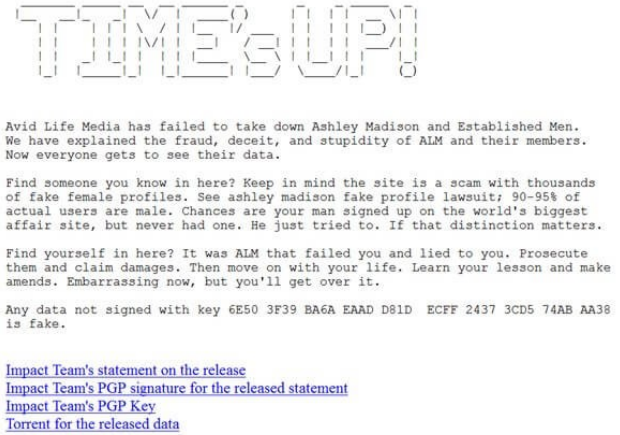
- Il sito si rivolge ad una clientela già sposata o in una relazione, promuovendo di fatto l'adulterio.

Attaccante: il gruppo "The Impact Team".

Il gruppo minaccia di divulgare le credenziali degli utenti se il sito non viene chiuso.

18-20 agosto: 25 GB di dati (incluse le credenziali degli utenti) è divulgato online.

Diversi utenti del sito si suicidano.



Ukraine's power grid cyber attack

(Leaving lots of people without electricity)

Dicembre 2015: viene condotto con successo il primo attacco cibernetico ad una rete elettrica.

I sistemi informativi di tre società ucraine di distribuzione elettrica sono violati.

230000 persone rimangono senza corrente elettrica per 6 ore.

Attaccante: [redacted].

DNC email leak

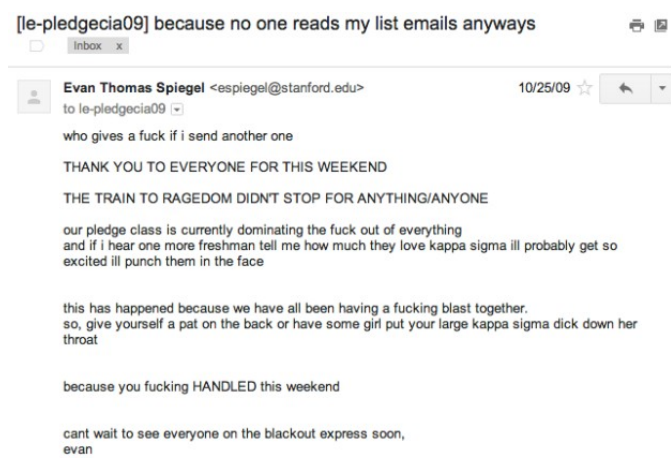
(Wreaks havoc on the Democratic Party)

22 luglio 2016: Wikileaks pubblica 19252 e-mail di personale affiliato al Democratic National Commitee (DNC), l'organo di governo del Partito Democratico statunitense.

Contenuti: interazioni del DMC con i media, campagne di Clinton/Sanders, finanziamenti, informazioni sensibili di alcuni dirigenti.

Conseguenze: 4 dirigenti del DNC si dimettono.

Attaccante: GucciFer 2.0 (tramite APT).



[le-pledgecia09] because no one reads my list emails anyways

Inbox x

Evan Thomas Spiegel <espiegel@stanford.edu> 10/25/09

to le-pledgecia09

who gives a fuck if i send another one

THANK YOU TO EVERYONE FOR THIS WEEKEND

THE TRAIN TO RAGEDOM DIDN'T STOP FOR ANYTHING/ANYONE

our pledge class is currently dominating the fuck out of everything
and if i hear one more freshman tell me how much they love kappa sigma ill probably get so excited ill punch them in the face

this has happened because we have all been having a fucking blast together.
so, give yourself a pat on the back or have some girl put your large kappa sigma dick down her throat

because you fucking HANDLED this weekend

cant wait to see everyone on the blackout express soon,
evan

USA elections interference

(No comment!)

Gennaio 2017: gli USA nutrono forti sospetti su una interferenza cibernetica durante le elezioni del 2016.

- Campagna di disinformazione tramite fake news, DNC leak.

Obiettivo: favorire la vittoria di Donald Trump su Hillary Clinton.

Attaccante: forti sospetti su Fancy Bear e Cozy Bear (due collettivi di hacker).

Mandante: [redacted].

I fratelli Occhionero

(Hanno controllato i potenti italiani per anni)

Gennaio 2017: i due fratelli Giulio e Francesca Maria Occhionero sono arrestati per spionaggio.

Usando un software complesso (EyePiramid), hanno infettato e monitorato per diversi anni i dispositivi (telefonini, PC, portatili) di politici, imprenditori, istituzioni e pubbliche amministrazioni.

Mandante: [redacted].

Il crollo di Equifax (2017)

(Long live CVE-2017-5638!)

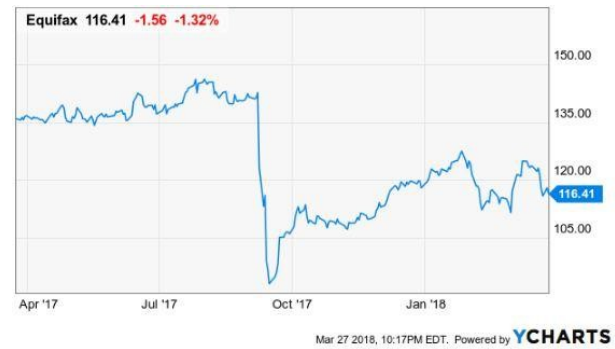
Nel 2017 la società di Big Data analytics Equifax è soggetta a molteplici attacchi.

Marzo: un malfunzionamento di Apache Struts permette l'ingresso nei sistemi.

Maggio-Luglio: vengono sottratte informazioni personali di 44 milioni di utenti.

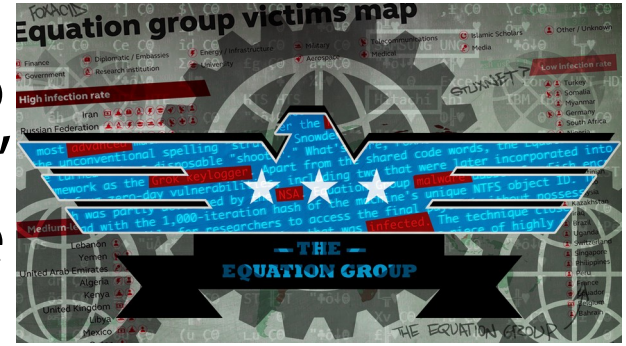
Ottobre: il sito Web espone malware.

Equifax non è stata ancora sanzionata ufficialmente, ma ha perso reputazione.



The Shadow Brokers (2016-2017)

(They hacked the NSA! They released ETERNALBLUE, AKA MS17-010!)



Nel 2016, il collettivo di hacker noto con il nome di “The Shadow Brokers” riesce a trafugare documenti e software usati dall’”Equation Group” della NSA.

- Tra questi figurano molti attacchi non noti per firewall, antivirus, Windows!

Agosto 2016-aprile 2017: cinque grandi campagne di pubblicazione.

Mandante: [redacted] .

Ransomware (2017)

(WannaCry)

Maggio 2017: il ransomware WannaCry si diffonde su scala mondiale, criptando e rendendo inutilizzabili centinaia di migliaia di macchine operanti servizi di pubblica utilità.

- Ospedali, telco, banche, governi, atenei

Viene chiesto un riscatto in bitcoin per lo sblocco.

Utilizza l'exploit ETERNALBLUE per riprodursi.

Mandante: [redacted].

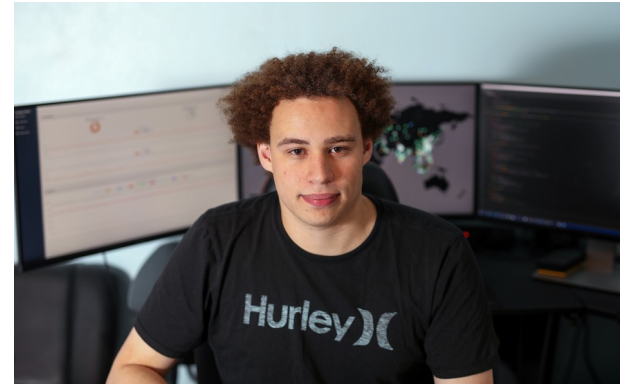
Marcus Hutchins (1994-)

(AKA “MalwareTech”; stopped WannaCry, was detained for that)

12 maggio 2017: un giovane ricercatore inglese (Marcus Hutchins AKA “MalwareTech”) trova un modo brillante di bloccare Wannacry (slide seguente).

Agosto 2017: Hutchins è arrestato a Las Vegas durante DEFCON, con l’accusa di aver scritto il malware bancario Kronos nel 2014/2015.

Luglio 2019: Hutchins è condannato ad un anno di libertà vigilata.



Il blocco di Wannacry

(One comic strip is worth a thousand words)

Ransomware (2017)

(NotPetya, Nyetya, Goldeneye)

Circa un mese dopo WannaCry viene lanciata una nuova campagna di attacchi con ransomware più sofitsticati di WannaCry (NotPetya, Nyetya, Goldeneye).

Vittime:

- diverse società in tutto il mondo
- Infrastrutture critiche dell'Ucraina

Mandante: [redacted].

CIA Vault 7 (2017)

(CIA's cyber warfare arsenal exposed)

Febbraio-settembre 2017: Wikileaks pubblica in 24 parti separate i documenti contenenti l'arsenale di armi cyber a disposizione della CIA.

Date dei documenti: 2013-2016.

Sistemi coinvolti: macchine, smart TV, Web browser, sistemi operativi.

Gola profonda (whistleblower): l'ingegnere Joshua Adam Shulte della CIA.

Macron campaign hack (2017)

(Destabilizing western democracy since 2016)

5 maggio 2017: due giorni prima del voto finale, ~20000 e-mail (9GB) del partito del candidato Emmanuel Macron sono pubblicate dal collettivo di hacker **Fancy Bear** (**APT28**).

Obiettivo: screditare il futuro presidente senza dargli la possibilità di replicare.

Mandante: [redacted].

Il disastro "Strava" (2018)

(Revealing classified military locations)

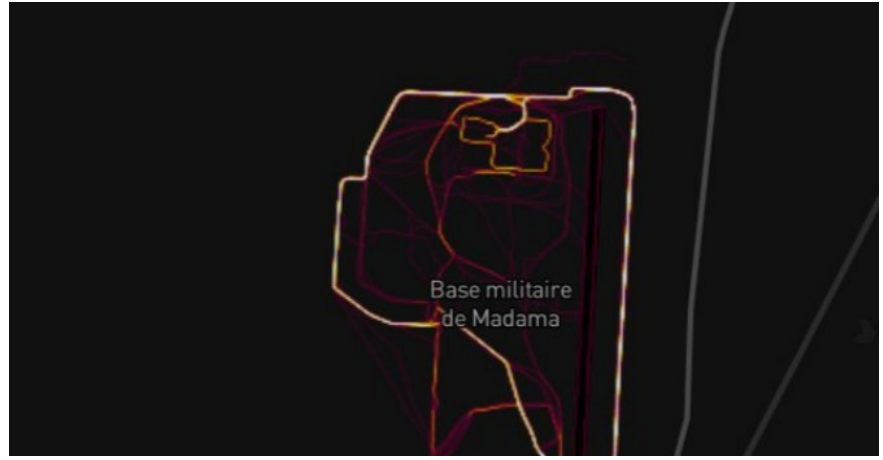
Novembre 2017: Strava, una popolare applicazione di fitness tracking, rilascia in pubblico la "heatmap" di tutti i percorsi svolti dai suoi utenti del 2017.

- 13000 miliardi di coordinate GPS relative a punti di percorsi di allenamento (tipicamente, corsa)

Il disastro "Strava" (2018)

(Revealing classified military locations)

Gennaio 2018: uno studente ventenne della National University di Canberra, Nathan Ruser, partendo dai percorsi di allenamento dei militari riesce ad identificare le installazioni militari segrete di mezzo mondo.



USA university hack (2018)

(Stealing intellectual property since 2013)

Marzo 2018: 9 hacker appartenenti alla stessa nazione esfiltrano dati da più di 300 istituzioni americane.

- 31 TB di dati sottratti
- 3 miliardi di dollari di proprietà intellettuale

Mandante: [redacted].

Data breach importanti (2018)

(Your data was probably stolen in 2018)

Starwood Hotels: 500M record
British Airways: 380K record (con carte di credito)
MyFitnessPal: 150M record (credenz.)
Facebook: 30M+ record (relazioni)
Mandante: [redacted]

Data breach importanti (2019)

(Your data was ~~probably~~ stolen in 2019)

Facebook: 540M+ record (relazioni)

Capital One: 140K SSN, 80K bank account

Quest Diagnostic: 11.9M record (test clinici)

Canva: 139M record (credenz., geolocalizzazione)

First American: 885M record (credenz., SSN, documenti)

Mandante: [redacted]

Twitter account hijack (2020)

(Greatest hack to a social media platform ever)

15 luglio 2020: un gruppo di attaccanti effettua un attacco di social engineering contro i dipendenti di Twitter e riesce ad accedere agli strumenti interni di gestione, aggirando la 2FA.

Ben 130 account di alto profilo sono violati ed usati per promuovere scam bitcoin. Il guadagno netto è 110K$.

31 luglio 2020: tre individui vengono arrestati.

Twitter account hijack (2020)

(I responsabili dell'hack)

Graham Ivan Clark: la mente dietro l'attacco.

Diciassettenne di Tampa (FL, USA) con una passione per gli hack su Minecraft.

Viene accusato di frode telematica, riciclaggio di denaro, furto di identità e accesso abusivo a diversi sistemi informatici.

Patteggia tre anni di carcere minorile.

Graham Ivan Clark
(2003-)

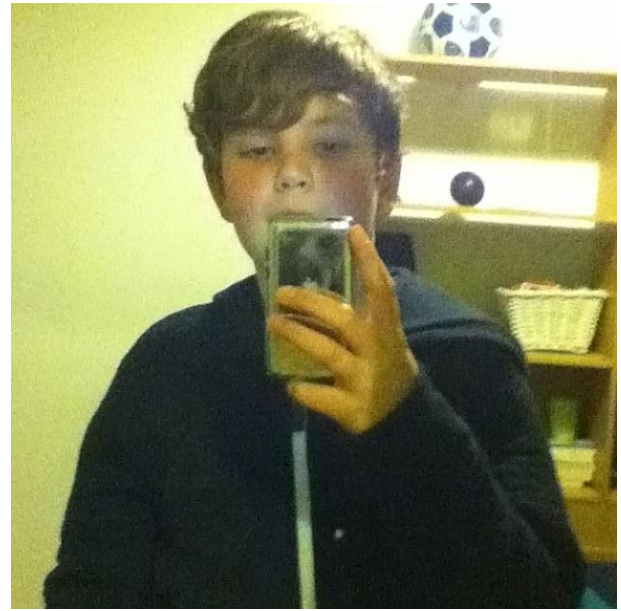
Twitter account hijack (2020)

(I responsabili dell'hack)

Mason Shepperd AKA "Chaewon": diciannovenne di Bognor Regis (UK). Gestisce uno dei cluster bitcoin coinvolti e vende account Twitter.

Viene accusato di associazione a delinquere finalizzata alla frode telematica, al riciclaggio di denaro e all'accesso abusivo a sistema informatico.

Viene arrestato ed è in attesa di estradizione verso gli US.



Mason Shepperd
(2001-)

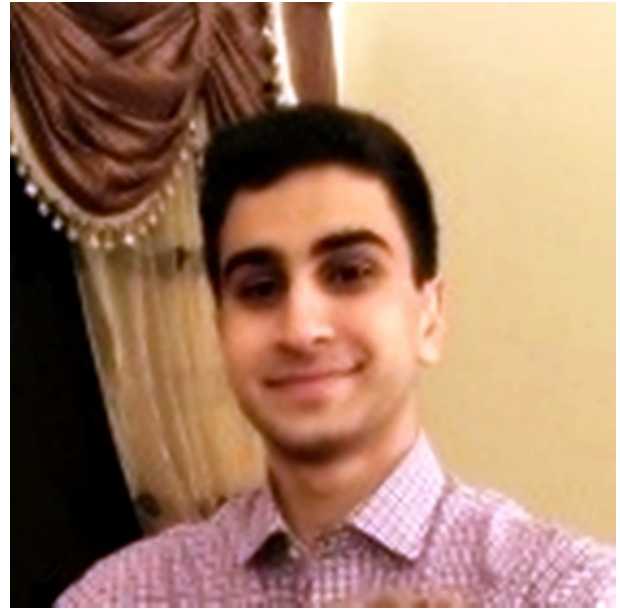
Twitter account hijack (2020)

(I responsabili dell'hack)

Nima Fazeli AKA "Rolex":

ventiduenne di Orlando (FL, US). Viola un sistema e vende account Twitter.

Viene accusato di accesso abusivo a sistema informatico. Il processo è tuttora in corso.



Nima Fazeli
(1998-)

Solarwinds hack (2019-2020)

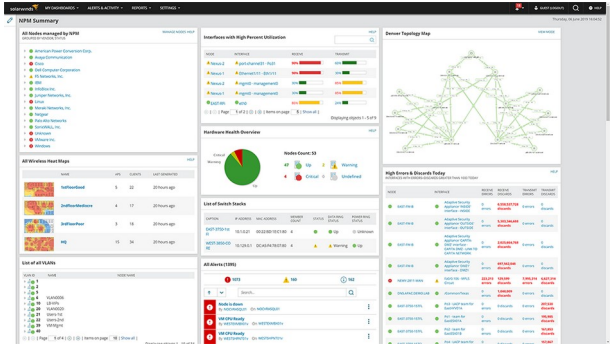
(La premessa)

SolarWinds è una ditta software che produce software di gestione dei sistemi (in primis, **Orion**).

Orion ha bisogno di accesso privilegiato ai sistemi che gestisce.

Orion è installato su diversi sistemi mission critical.

→ Orion è un obiettivo succulento per gli attaccanti.



SolarWinds hack (2019-2020)

(L'attacco)

Settembre 2019: gli attaccanti ottengono accesso alla rete interna di SolarWinds.

Ottobre 2019: gli attaccanti provano ad iniettare codice in Orion.

20 febbraio 2020: il trojan Sunburst è iniettato nel software Orion.

26 marzo 2020: SolarWinds distribuisce ai propri clienti il software con le modifiche maliziose.

SolarWinds hack (2019-2020)

(Supply chain attack)

L'hack SolarWinds, unito a Sunburst, rappresenta un classico esempio di **attacco alla filiera di fornitura** (**supply chain attack**).

Non si attacca direttamente il sistema vittima, bensì un componente esterno fornito da una terza parte.

→ Gli aggiornamenti del componen-te esterno possono introdurre vere e proprie "backdoor" di accesso.

→ Backdoor difficili da individuare se si controlla solo il sistema vittima.

SolarWinds hack (2019-2020)

(Mandante e vittime illustri)

Dicembre 2020: FireEye scopre l'attacco, lo descrive e divulga un elenco di vittime.

Mandante: [redacted]

Vittime illustri: FireEye, diversi dipartimenti US e UK, NATO, parla-mento europeo, AstraZeneca.

Microsoft Exchange Hack (2021)

(Ovvero, usare Windows remoti gratis e senza credenziali)

Gennaio 2021: viene scoperto un attacco che, sfruttando difetti non noti pubblicamente, consente di ottenere accesso a Microsoft Exchange con credenziali di amministratore.

È possibile leggere le email.

È possibile installare backdoor per il futuro accesso.

È possibile eseguire ransomware (DearCry).

Vittime illustri: di tutto e di più.

Mandante: [redacted]

Colonial pipeline hack (2021)

(Ovvero, come privare gran parte degli US di petrolio)

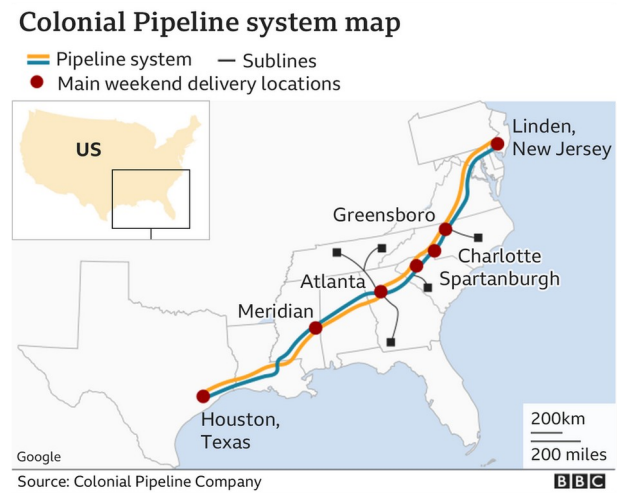
Maggio 2021: **Colonial Pipeline**, un oleodotto che serve il sud-est degli US, è vittima di un ransomware.

L'impianto è messo fuori uso.

Vengono richiesti 75 bitcoin (4.4M USD) per l'ottenimento delle chiavi di decifratura.

Una volta pagato il riscatto, il sistema è stato ripristinato.

Mandante: [redacted]



Log4Shell (2021)

(Ovvero usare UNIX e Windows remoti gratis e senza credenziali)

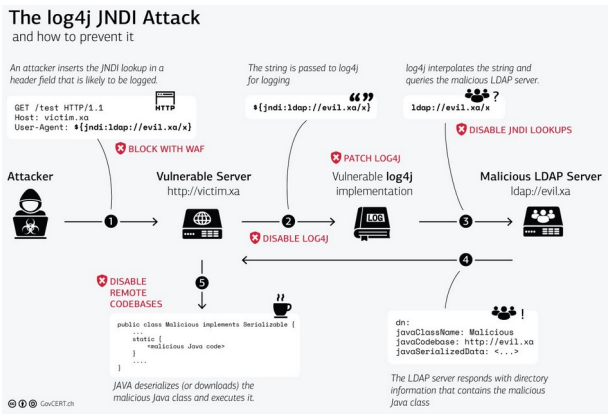
Log4J è uno dei framework più popolari per il logging in Java.

Dicembre 2021: Chen Zhaojun (team di sicurezza di Alibaba) divulga una vulnerabilità in Log4J che consente l'esecuzione remota di codice arbitrario senza autenticazione.

Il problema persiste dal 2013!

Vittime illustri: AWS, Cloudflare, iCloud, Steam, Tencent QQ, …

Log4Shell è da molti ritenuta la vulnerabilità più grave di sempre.



Lessons learned

(The meaning of the term "hacking" has changed; watch your language)

Il termine "hacking" ha cambiato radicalmente significato nel tempo. È sempre bene specificarne il contesto.

tempo

burla innocente (prank), volta a dimostrare la propria superiorità tecnica, di fantasia, di immaginazione.

procedura fantasiosa (più o meno illegale) per ottenere un piccolo lucro personale.

procedura sempre più fantasiosa ed illegale per ottenere un grande lucro.

complesso insieme di attività volto a controbattere un'ingiustizia sociale.

complesso insieme di attività volto a conseguire un vantaggio strategico politico e/o industriale.

Lessons learned

("Hacking" MIT-style requires a peculiar set of skills; it ain't that easy, dudes...)

L'hacking in stile "MIT Tech Railroad Club" richiede un insieme di abilità non comuni.

- Curiosità intellettuale.
- Passione sfrenata (maniacale?) per la materia di interesse.
- Conoscenza completa del contesto (hardware, software).
- Pensiero laterale.
- Voglia di emergere.

Queste abilità non si imparano (solo) a scuola.

Lessons learned

("Hacking"black-hat style will likely get you to prison)

L'hacking in stile "black hat" finisce quasi sempre nello stesso modo.

- Una denuncia, un processo, una condanna penale.

Per imparare a difendersi, è necessario imparare anche ad attaccare. È di fondamentale importanza allenarsi in maniera legale.

- Macchine virtuali sul proprio portatile.
- Servizi su cui si ha autorizzazione per operare.

Lessons learned

(Being a lone dog won't get you very far)

La complessità in materia di sicurezza è tale da essere ingestibile da un singolo individuo.

Che sia attacco oppure difesa…

La sicurezza è, ormai, un **processo industriale**.

Noi tutti siamo parte di quel processo.

Bisogna imparare a collaborare con altri professionisti.

Lessons learned

(Defending is much more challenging than **attacking**)

All'attaccante può bastare una singola falla per poter violare una infrastruttura tecnologica.

L'attaccante ha il vantaggio di poter scegliere metodi ed obiettivi dell'attacco.

L'attaccante è più appetibile per i media (è spesso visto come un eroe).

Gli strumenti a disposizione dell'attaccante sono spesso un passo in avanti.

Lessons learned

(**Defending** is much more challenging than attacking)

Il difensore deve individuare tutte le falle e ripararle.

Il difensore non ha il lusso di scegliere le regole del gioco; deve adattarsi all'attaccante.

Il difensore non è appetibile ai media (è spesso menzionato se fallisce clamorosamente).

Il difensore può doversi scontrare con tecniche e strumenti mai impiegati in precedenza.

Lessons learned
(Targets are manyfold)

Gli obiettivi di un attaccante sono molteplici.

- Un apparato hardware.
- Un software (SO, libreria, applicazione).
- Una procedura/algoritmo.
- Una persona.

Nella sua attività quotidiana, un programmatore deve costantemente tenere in conto minacce ed obiettivi.

Lessons learned

(History repeats!)

La storia si ripete.

Gli errori commessi sono sempre gli stessi.

Le risposte agli incidenti di sicurezza sono sempre le stesse.

Il programmatore ha a sua disposizione una grande arma: la storia!

Che gli insegna quello che NON deve fare.