Gli attacchi hacker più famosi della storia.

I 10 virus informatici che hanno sconvolto il mondo digitale

La diffusione di Internet è stata una delle rivoluzioni storiche più importanti da quando l'uomo ha mosso i primi passi sulla Terra, ma ha anche comportato gravi rischi.
Gli attacchi informatici sono oggi episodi estremamente frequenti nonostante le contromisure adottate.

2020 nel mondo

+390%
rispetto al 2019

un attacco informatico ogni
11 secondi

2020 in Italia

+667%
rispetto al 2019

un attacco informatico ogni
19 secondi

Ripercorriamo insieme la storia degli attacchi informatici più importanti degli ultimi 40 anni.

1982
Cyber attacco durante la Guerra Fredda

Nel 1982 la **CIA** riuscì ad introdursi nei sistemi di un **gasdotto siberiano**, installando un codice che mandò in panne i sistemi di controllo delle pompe del gas, causando un aumento di pressione e la conseguente esplosione dell'intera centrale energetica. Fu **la più grande detonazione non nucleare della storia**. La prima dimostrazione della potenza di uno **logic bomb**[1] azionata con un semplice click.

1988
Il malware nato per errore

R. T. Morris, studente della **Cornell University**, sviluppò come esperimento accademico un worm, un malware capace di autoreplicarsi. Quando il virus fu immesso in rete produsse però un errore e anda a infettare oltre 6000 computer, provocando **danni per circa 100 milioni di dollari**. Il worm si replicava centinaia di volte negli stessi computer, sovraccaricandoli la loro memoria e portando i processori al collasso. Nonostante si trattasse di uno sbaglio le autorità americane arrestarono il giovane studente **fu la prima condanna per pirateria informatica negli Stati Uniti**.

1999
Un sedicenne conquista la NASA

J. J. James è stato il **primo hacker minorenne incarcerato** per un crimine informatico negli Stati Uniti, condannato per aver illegalmente ottenuto dal computer della **NASA** e degli uffici del **Pentagono**. L'adolescente spse migliaia di e-mail e documenti militari riservati riuscendo inoltre ad impossessarsi di alcuni codici di un programma della NASA. Ciò costrinse la Stazione Spaziale a ripristinare i propri sistemi spendendo circa **1,7 milioni di dollari** per liberarsi definitivamente dal virus.

2000
Il virus romantico ILOVEYOU

Noto virus installato tramite posta elettronica. L'Utente riceveva un'e-mail con oggetto "ILOVEYOU" e un allegato appaiamente in formato testuale chiamato **"LOVE-LETTER-FOR-YOU.TXT.vbs"**. Il file in realtà nascondeva un trojan che appena aperto andava a rubare informazioni sensibili. Il worm inviava inoltre una copia di se stesso a tutti i contatti presenti in rubrica, cosicché i mittenti spesso apparivano come conoscenti e venivano pertanto considerati affidabili. La diffusione partì dalle **Filippine** spostandosi verso ovest fino agli **Stati Uniti**. Furono stimati danni da **5,5 miliardi di dollari** con **50 milioni di computer infettati**.

2006
Shady RAT

Un virus che ha lavorato di nascosto diffondendosi via mail per ben cinque anni, scoperto solamente nel 2011. Una volta installato sul computer, **Shady RAT** era in grado di leggere diversi file memorizzati nel sistema. Questa operazione colpì 79 organizzazioni di 14 nazioni diverse comprese le **Nazioni Unite, l'Agencia Mondiale Anti-Doping e il Comitato Olimpico Internazionale**. Dal 2006 furono trafugati centinaia di documenti considerati top secret. Non è mai stato scoperto chi ci fosse dietro questa organizzazione di hacker e nemmeno gli scopi dell'operazione.

2009
Operazione Aurora

A metà del 2009, sfruttando due falle nel sistema di controllo del server **Google**, diversi dati preziosi riuscirono ad accedere illecitamente alla banca dati di multinazionali americane, organi di sicurezza e difesa militare. Questa operazione denominata "**Aurora**" secondo i vertici Google era stata guidata dal governo di Pechino, molti account Gmail compromessi appartenevano ad attivisti americani, europei e cinesi impegnati a difendere i diritti umani nel paese asiatico. La scandalo ebbe ovviamente dei risvolti politici ed evidenziò le lacune del sistema di sicurezza Google.

2009
Stuxnet

Stuxnet è un virus informatico creato e diffuso dal Governo statunitense in collaborazione col governo israeliano. Lo scopo del software era il **sabotaggio della centrale nucleare iraniana** di Natanz. Il virus infettò per anni il programma nucleare del paese e venne scoperto solamente quando il malware si diffuse al di fuori dello stabilimento, probabilmente tramite un PC portatile infetto. Furono colpite in larvato tempo aziende giapponesi, europee ed americane da cui provenivano le attrezzature per il programma atomico iraniano. Tutto fin così sotto l'attenzione dei media mondiali e dell'opinione pubblica.

2012
Darkhotel

Questo attacco ha colpito top manager di multinazionali e personalità istituzionali che hanno soggiornato in **hotel lussuosi in Asia**. Le vittime, quando si collegavano alla rete aperta dell'hotel, ricevevano notifiche di aggiornamento del software del proprio dispositivo. In questo modo si annidava nel sistema il virus spyware **DarkHotel**, installato da cybercriminali di registrare in segreto i tasti digitati dalla vittima così da spiare canali di comunicazione, rubare password e altre informazioni riservate. Gli hacker sfruttavano i dati solo dopo 180 giorni per non destare sospetti.

2012
Anonymous vs Vaticano

Il gruppo di hacker più celebre al mondo il 17 marzo 2012 rese inagibile per due giorni il **sito del Vaticano**. I membri di **Anonymous** ritenevano che nel XXI secolo non fosse ammissibile ancora la discriminazione religiose, sessuali o politiche, portate avanti secondo loro dalla Chiesa. I gruppi informatici criticavano in particolare la scelta della Santa Sede di proibire la sperimentazione su cellule staminali per la ricerca della cura di molte malattie mortali.

Una settimana più tardi, Anonymous hackerò il database di **Radio Vaticana** in segno di protesta per aver usato ripetitori con potenza di trasmissione fuori dai limiti di legge, emettendo onde elettromagnetiche causa di gravi malattie.

Ancora una settimana più tardi il sito del Vaticano tornò off-line. Il gesto voleva portare in risalto la presunta omertà da parte del Papa nei non denunciare casi di pedofilia.

2014
Hacker alla conquista del cinema

Il gruppo hacker "**I guardiani della pace**" sferrò un cyber attacco contro **Sony Entertainment** diffondendo dati sensibili dei propri dipendenti (conversazioni email, informazioni finanziarie), film non ancora uscì e progetti di nuove pellicole. Il motivo scatenante fu l'annuncio dell'uscita del film "The interview" che narra la storia di due giornalisti americani intenti ad assassinare il leader nord-coreano Kim Jong-un.

Gli hacker minacciarono inoltre attacchi terroristici nelle sale che avrebbero proiettato il film. The Interview per questo uscì solo in 200 sale indipendenti e su alcune piattaforme streaming.

A cura della
Facoltà di Ingegneria Informatica dell'Università Niccolò Cusano

UNIVERSITÀ NICCOLÒ CUSANO

Fonti

https://www.panorama.it/cosa-fra-lo-58-terrasacco-cosa-sappiamo-delle-armi-sul-cacciatore-degli-hacker-siberia/
https://www.insurtechnews.it/gli-5-attacchi-hacker-piu-famosi-della-storia/
https://www.avast.it/unique-attacks-hacker-piu-pericolosi-della-storia-dell#topic-0/
https://www.ultimaora.com/stuxnet-virus-iran-nucleare/
https://www.bitdrink.it/blog/news/gli%27gli-attacchi-informatici-piu-importanti-degli-ultimi-30-anni
https://www.cnn.com/2012/03/16/tech/anonymous-vatican-web-bomb/
https://www.kaspersky.it/blog/darkhotel-spy-hotels/
https://www.kaspersky.it/blog/darkhotel-spy-hotels/
https://www.ansa.it/sito/notizie/cronaca/2014/12/19/hacker-minaccia-usa-stroncherebbe-definitivamente-sony-pictures-hackerata-sony-pictures-dati-dipendenti-sceneggiature-film-non-ancora-usciti-progetti-di-nuove-pellicole_1.html#:~:text=Il%20%22gruppo%20hacker%20%22,%20%22Guardiani%20della%20Pace%22.
https://it.wikipedia.org/wiki/Anonymous
https://www.treccani.it/enciclopedia/cronologia-dei-cyberattacchi-dal-1982-al-2020_(Enciclopedia-dei-ragazzi)/
https://www.wikiwoo.com/hacker-e-crimi-in-attacco-informatico-ogni-10-secondi_2012-07-05.html#:~:text=Ogni%20%2C%20%2C%20%2C