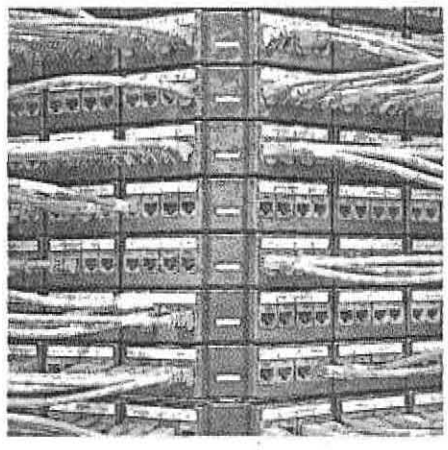
La guida

PER SAPERNE DI PIÙ
https://www.commissariatodips.it
www.repubblica.it

Come difendersi



Posta sospetta e file sconosciuti: le armi dei pirati del web

Domande & risposte

ATTACCHI COME QUELLI SUBITI DALLE PIÙ ALTE CARICHE DELLO STATO POSSONO CAPITARE OGNI GIORNO A CHIUNQUE. COME AVVENGONO?
Chi vuole spiare i nostri dati personali ci invia, da account fasulli, un messaggio, quasi sempre sulla nostra posta elettronica, nel quale chiede di scaricare un allegato oppure di aprire un link. Nel primo caso, basta scaricare l'attachment per far entrare gli hacker nel proprio device. Nel secondo, invece, si viene reindirizzati perlopiù a una pagina fake, identica a quella originale, del proprio gestore di posta elettronica (gmail, yahoo, eccetera), nel quale ci viene chiesto di inserire le nostre credenziali. A quel punto gli hacker sono nel nostro computer.

L'AGGANCIO
Chi vuole spiare i nostri dati ci invia, da account fasulli, un messaggio sulla posta elettronica

LE MAIL VENGONO INVIATE DA INDIRIZZI SCONOSCIUTI?
La maggior parte delle volte no. Alla base c'è un lavoro di profiling da parte degli hacker. Sfruttando informazioni aperte, come per esempio quelle presenti sui social network, cercano di capire quali sono le nostre passioni (squadre di calcio, shopping) o gli amici con i quali si è in contatto più frequentemente. Ed è da account di questo tipo che arrivano le mail spia.
«Ormai — spiega Andrea Zapparoli Manzoni, uno dei principali esperti di sicurezza informatica in Italia — non siamo più abituati a dubitare di quello che c'è su Internet. Ci fidiamo, per esempio, delle identità. Quello del phishing è un fenomeno che non colpisce il sistema informatico quanto la nostra psicologia: è un'attività di ingegneria sociale che porta all'alterazione della percezione. Se la vittima avesse chiaro quello che sta succedendo, non darebbe mai le proprie credenziali. E invece molto spesso accade».

LA TECNICA
Il phishing è un'attività di ingegneria sociale che porta alla alterazione della percezione

QUALI SONO LE CONTROMISURE?
Bisogna prestare grande attenzione al messaggio contenute nelle mail. I testi hanno sempre delle caratteristiche strane. Per questo prima di aprirle bisognerebbe farsi delle domande: il mittente è quello che sembra? Ha senso che mi scriva in quella maniera? L'allegato che mi ha mandato lo apro direttamente o lo passo prima all'antivirus e poi lo faccio gestire da un software esterno? «In ogni caso — spiega la Polizia postale — non è possibile infettare il nostro computer leggendo semplicemente il testo di una mail ma è necessario eseguire il file infetto. Dunque, è importante prestare grande attenzione agli allegati».

I TELEFONINI
Sui telefoni in pochi hanno programmi antivirus in grado di individuare i malware

L'INFEZIONE PUÒ ARRIVARE SOLTANTO VIA MAIL?
No, sempre più spesso vengono utilizzati i social network. In chat arrivano link da aprire da profili che, nella maggior parte dei casi, hanno lo stesso nome, cognome e foto profilo di nostri amici reali. Anche in questo caso bisogna fare grande attenzione, quindi, prima di cliccare su un qualsiasi link.

POSSONO ESSERE COLPITI SOLTANTO I COMPUTER?
No, ogni device è potenzialmente vulnerabile. Gli smartphone soprattutto. «Sui telefoni — dice Zapparoli — non vedi quello che sta succedendo. E in pochi hanno programmi antivirus installati in grado di individuare i malware».

GLI ANTIVIRUS SONO UN BUONO STRUMENTO DI PROTEZIONE?
Sì. Purché, però, siano costantemente aggiornati. «Considerato che ogni giorno vengono creati nuovi virus — spiega ancora la Postale — e che, con lo sviluppo della Rete Internet, questi si diffondono con eccezionale rapidità, risulta fondamentale aggiornarlo. Un antivirus, se non aggiornato con regolarità, ci potrebbe far correre rischi maggiori rispetto al non averlo affatto, poiché ci potrebbe far sentire sicuri fino a trascurare le più elementari norme di sicurezza informatica».

CI SONO ALTRE MANIERE PER ACCORGERSI DEGLI ATTACCHI?
È importante verificare sempre gli Ip con i quali è stato effettuato l'accesso sulla posta elettronica o anche sui social network. In caso di dispositivi non riconosciuti è importante cambiare immediatamente la password e presentare denuncia alla polizia postale. Anche se, per sbaglio, si scarica un allegato o si comunicano propri dati personali è bene segnalarlo all'autorità giudiziaria. «Bisogna abituarsi a tenere distinti gli ambiti: non si può fare home banking, per esempio, sul computer in cui si scarica qualsiasi altra cosa» dice Zapparoli.

ESISTONO SISTEMI OPERATIVI INATTACCABILI?
No. Esistono però delle difficoltà diverse. «Ios, il sistema operativo di Apple — spiega ancora Zapparoli Manzoni — è sicuramente meno attaccabile perché è un sistema chiuso, perché ha molte meno versioni, ma questo non significa che sia invulnerabile». Certo, i prezzi sul mercato nero sono diversi. «Trovare un baco su Ios può valore un milione di dollari. Sugli altri sistemi operativi, anche 50mila euro».

A cura di
GIULIANO
FOSCHINI