Polizia di Stato

Polizia Postale e delle Comunicazioni - consigli utili

La Polizia Postale e delle Comunicazioni ha ricevuto in questi giorni numerosissime segnalazioni relative alla ricezione di strane mail, anche in inglese, che nell'oggetto riportano il nostro indirizzo di posta elettronica e la nostra password, attuale o passata e nel messaggio informano che, proprio grazie alla conoscenza della nostra password, il mittente, nascosto o con un nome di fantasia, sarebbe riuscito ad ottenere il controllo del nostro dispositivo e della webcam, ed avrebbe, successivamente, girato a nostra insaputa un filmato, che ci ritrarrebbe intenti a guardare film pornografici. Il messaggio prosegue con la minaccia di diffondere il presunto video intimo ad un elenco di nostri contatti (familiari ed amici), di cui disporrebbe grazie ad un precedente accesso abusivo ai nostri profili social nel caso in cui non si proceda al pagamento di un riscatto in bitcoin. L'offerta perentoria è stata inviata via mail a centinaia di indirizzi di imprenditori, vertici di aziende pubbliche e private, figure istituzionali, professori universitari. Con lo stesso messaggio e il medesimo terribile ricatto e con richieste che sono arrivate fino a 5.000 dollari. E' comprensibile come questa situazione abbai gettato nel panico i destinatari delle mail, considerato che la password corrisponde a quella utilizzata e che la minaccia della diffusione di video privati ipotizza uno scenario imprevedibile e destabilizzante. Le centinaia di mail inviate a pioggia in tutta Italia hanno creato un vero allarme diffuso tra cittadini e personaggi pubblici. Diverse le reazioni, numerose le denunce ma molte anche le persone che, per la paura della diffusione dei "fantomatici" video, restano nel silenzio. Attenzione: nulla di tutto ciò è reale. La Polizia Postale e delle Comunicazioni, infatti, ha accertato che si tratta "semplicemente" dell'ultima modalità con la quale criminali informatici senza scrupoli tentano di costringere i malcapitati a subire una vera e propria cyber-estorsione. L'unico elemento autentico dell'intera vicenda è rappresentato proprio dalla password - anche precedente e da noi non più utilizzata - del nostro account virtuale, password della quale i criminali in questione sono entrati in possesso sfruttando, presumibilmente, i numerosi mercati neri presenti sul *darkweb*. Tutto il resto, invece, rappresenta un'invenzione dell'autore del reato, elaborata al solo scopo di gettarci nel panico ed indurci a pagare la somma illecita: è tecnicamente impossibile, infatti, che chiunque, pur se entrato abusivamente nella nostra casella di posta elettronica, abbia potuto - per ciò solo – installare un virus in grado di assumere il controllo del nostro dispositivo, attivando la webcam o rubando i nostri dati. Ecco dunque alcuni consigli su come comportarsi:

° Mantenere la calma: Il criminale non dispone, in realtà, di alcun filmato che ci ritrae in atteggiamenti intimi né, con tutta probabilità, delle password dei profili social da cui ricavare la lista di nostri amici o parenti

- Non pagare assolutamente alcun riscatto: l'esperienza maturata con riguardo a precedenti fattispecie criminose (come *sextortion* e *ransomware*) dimostra che, persino quando il criminale dispone effettivamente di nostri dati informatici, pagare il riscatto determina quale unico effetto un accanimento nelle richieste estorsive, volte ad ottenere ulteriore denaro
- Proteggere adeguatamente la nostra email (ed in generale i nostri account virtuali): cambiare - se non si è già provveduto a farlo - la password, impostando password complesse; non utilizzare mai la stessa password per più profili; abilitare, ove possibile, meccanismi di autenticazione "forte" ai nostri spazi virtuali, che associno all'inserimento della password, l'immissione di un codice di sicurezza ricevuto sul nostro telefono cellulare
- Tenere presente che l'inoculazione (quella vera) di virus informatici capaci di assumere il controllo dei nostri dispositivi può avvenire soltanto se i criminali informatici abbiano avuto disponibilità materiale dei dispositivi stessi, oppure qualora siano riusciti a consumare, ai nostri danni, episodi di *phishing informatico:* è buona norma quindi non lasciare mai i nostri dispositivi incustoditi (e non protetti) e guardarsi dal cliccare su link o allegati di posta elettronica sospetti
- Aggiornare sempre il sistema operativo dei nostri dispositivi, ed installare e tenere aggiornati adeguati sistemi antivirus

25/07/2018