Operazione “Rear Window” della Polizia postale di Milano

Spiavano le persone direttamente nelle loro case, nelle stanze d’albergo, negli studi medici e negli spogliatoi delle palestre introducendosi attraverso il wifi nelle telecamere installate per la videosorveglianza. La Polizia postale di Milano ha denunciato 10 persone ed eseguito altrettante perquisizioni in diverse città italiane su disposizione della procura di Milano, a conclusione di un’indagine chiamata “Rear Window”.

Gli investigatori sono riusciti ad individuare i componenti di due gruppi criminali, per uno dei quali si configura l’associazione per delinquere; gli indagati riuscivano ad “introdursi” illegalmente violando la privacy di ignare persone con sofisticati sistemi informatici che permettevano loro di scandagliare la Rete alla ricerca di impianti di videosorveglianza connessi ad Internet. Una volta trovata la linea giusta, gli indagati effettuavano un attacco informatico che consentiva di scoprire le password degli Nvr (videoregistratori digitali a cui vengono collegate le telecamere).

Il principale scopo degli indagati era quello di vendere i filmati e le immagini captate nei momenti di intimità delle persone, su delle “vetrine” online create ad hoc.

I luoghi virtuali scelti dagli indagati nella speranza di rimanere anonimi erano il social network “?????????” (“VKontakte”, abbreviato VK, conosciuto come la versione russa di Facebook) e Telegram.

Al termine delle perquisizioni, gli investigatori della Postale di Milano, Napoli e Catania hanno sequestrato 10 smartphone, 3 workstation, 5 PC portatili, 12 hard disk e svariati spazi cloud, per una capacità di archiviazione complessiva di oltre 50 Terabyte. Sono stati inoltre sequestrati tutti gli account social usati dagli indagati e diverse migliaia di euro, anche in criptovaluta.

I consigli degli specialisti

Consigliamo sempre di affidarsi a professionisti affidabili nell’installazione di impianti di videosorveglianza ed evitare soluzioni “fai da te”. Ricordiamo che gli attuali sistemi di videosorveglianza sono a tutti gli effetti sistemi informatici connessi ad Internet e, come tali, sono esposti alle insidie della Rete e necessitano, quindi di costanti aggiornamenti software per eliminare vulnerabilità di sistema e, naturalmente, vanno configurati in maniera adeguata.

Ad esempio, è preferibile inibire l’accesso tramite Web per il controllo remoto delle telecamere e optare per sistemi “peer to peer” tramite cloud a patto però che ci si orienti verso dispositivi realizzati da primarie aziende del settore, evitando assolutamente prodotti acquistabili online a basso costo.

Inoltre, anche se può apparire scontato e banale, si raccomanda sempre di cambiare la password di default per l’accesso all’interfaccia di configurazione scegliendone una che contenga almeno otto caratteri, con lettere minuscole, maiuscole (possibilmente non all’inizio), numeri e caratteri speciali e orientare le telecamere in modo da non inquadrare bagni, camere da letto e altri ambienti “sensibili” per l’intimità delle persone.

08/06/2022