Rintracciato dalla Polizia postale l’hacker del “Covid19”

Lo scorso anno, proprio durante le prime fasi della pandemia da Covid19, un 45 enne della provincia di Taranto ha messo in piedi una campagna di spear phishing perpetrata attraverso l’invio massivo di mail ad ignare vittime, a cui rubava dati personali.

Nei giorni scorsi, a conclusione dell’indagine denominata “Glaaki”, i poliziotti della polizia postale hanno indagato l’uomo, un informatico esperto in codici di programmazione, per i reati di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici e diffusione di programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

L’indagato, infatti, con il pretesto di fornire aggiornamenti sull’avanzamento del contagio, inviava mail contenenti un codice malevolo, di tipo keylogger, usando come oggetto Covid19. Approfittando dello stato psicologico dovuto all’emergenza, è riuscito ad appropriarsi di password, credenziali bancarie e dati personali di chi spontaneamente apriva l’allegato infettato.

Una volta aperte le porte del sistema informatico della vittima, l’hacker estrapolava i contatti della rubrica della casella di posta elettronica, a loro volta potenziali vittime, ai quali inviava nuovi messaggi portatori del virus.

L’attività di analisi del traffico prodotto dal malware, dai computer violati verso altri spazi web, ha consentito, agli investigatori del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), e del compartimento polizia postale di Bari, di ricostruire il funzionamento del codice malevolo e quindi l’origine del traffico dati, fino ad arrivare all’individuazione di alcuni IP utilizzati dal 45enne.

Le indagini sono ancora in corso per accertare e individuare eventuali complici dell’uomo e i possibili acquirenti dei dati sottratti.

12/02/2021