Polizia di Stato

Polizia Postale di Triete: Operazione Cryptowash

La Polizia di Stato di Trieste ha concluso un'importante operazione dedita al riciclaggio e alle estorsioni on line mediante la diffusione del virus "Cryptolocker" denunciando 7 per i reati di accesso abusivo informatico, estorsione e riciclaggio degli illeciti proventi realizzati.Il criptolocker è un virus trasmesso via email apparentemente provenienti ad esempio da corrieri per le spedizioni o agenzie governative nazionali, contenenti link o allegati che una volta aperti cripano il contenuto delle memorie deicomputer, anche collegati in rete. Gli utenti, per riaprire il file, erano costretti a pagare un riscatto a fronte del quale veniva loro inviato via email un programma per la decriptazione.L'attività criminale in oggetto si era diffusa già da diversi sedi governative, come Tribunali, Uffici comunali e anche alcune strutture delle diverse sedi governative, come Tribunali, Uffici comunali e anche alcune strutture delle diverse Forze dell'Ordine.**L**e indagini degli uomini della Polizia Postale sono partite da una denuncia dell'amministratore delegato di una società in cui una impiegata aveva incautamente aperto un link, pervenuto in allegato a una email che preannunciava un rimborso su una spedizione SDA. Una volta aperto il link, è stato in realtà scaricato il "Cryptolocker", che ha criptato il contenuto delle memorie dei pc aziendali. I responsabili della ditta seguendo le istruzioni fornite dai criminali, pagavano il riscatto e ricevevano per posta elettronica il file che consentiva il ripristino dei dati sui computer aziendali. Partendo da queste informazioni, il personale della Polizia Postale individuava una persona in provincia di Padova riconducibile a un vero e proprio sodalizio i cui appartenenti si presentavano come semplici intermediari di coinbit che non solo si dichiaravano estranei alla diffusione del virus ma anzi sui propri siti invitavano le malcapitate vittime a non pagare alcun riscatto in caso di attacco bensì a sporgere denuncia presso la Polizia Postale. In realtà erano perfettamente al corrente della natura illecita dei proventi incamerati poiché la Polizia Postale trovava le tracce non solo delle transazioni effettuate a seguito del pagamento dei riscatti ma addirittura recuperava centinaia di messaggi che gli indagati si inviavano via smartphone. In questi messaggi si scambiavano consigli sulla diffusione del cryptolocker, sul riciclaggio del denaro, su come comportarsi davanti alle forze di polizia in caso di perquisizione o di assunzione di sommarie informazioni, indicazioni su nomine di avvocati di fiducia e altro. Erano messaggi del tipo:"Cercate di essere vaghi… E dire il meno possibile", "Se non avete un avvocato di fiducia potete usare avv……","devo fare un cryptolocker pure io", "un acquisto ora, 2 giorni fa un altro" e "oggi già 3 scaldate gli avvocati", dal tenore dei quali si evince la consapevolezza che il prezzo pagato delle transazioni è in realtà il prezzo pagato dalle vittime dell'estorsione per ottenere il programma per decriptare i file. Numerose le perquisizioni che hanno portato al sequestro di computer, hard disk, tablet, pen drive usb, smartphone, carte di credito e documentazione ritenuta utile per il proseguimento delle indagini.

08/07/2015