Scritto da Red.
Giovedì 11 Febbraio 2016 10:50



AVELLINO – La polizia postale e delle comunicazioni ha registrato un'ondata di attacchi attraverso l'invio di mail contenenti il già noto virus "*Cryptolocker*" che imperversa, con maggiore frequenza, già da un po' di tempo sul web. Purtroppo – si legge in un comunicato – nonostante le attività investigative abbiano consentito di individuare persone e gruppi organizzati, sia italiani che stranieri responsabili di questi attacchi, la estesa diffusione del fenomeno e la costante per cui l'attacco si rileva possibile, sempre e comunque, grazie ad un comportamento disattento e superficiale dell'utente, hanno indotto la polizia di Stato ad aumentare le misure di prevenzione attraverso ogni strumento utile a garantire la sicurezza di chi naviga in rete.

Lo scenario è il seguente: l'ignaro utente riceve sulla propria casella di posta elettronica un messaggio che fornisce indicazioni ingannevoli su presunte spedizioni effettuate, oppure contenente un link o un allegato a nome di istituti di credito, aziende, enti e/o gestori di servizi noti al pubblico. Cliccando sul link oppure aprendo l'allegato - solitamente in formato pdf, zip) - viene istantaneamente iniettato un virus che nel giro di pochi secondi cripta il contenuto delle memorie dei computer, anche di quelli eventualmente collegati in rete, rendendo inutilizzabile l'utilizzo dei propri file. A questo punto si realizza il ricatto dei criminali informatici che richiedono agli utenti, il pagamento di una somma di denaro di alcune centinaia di euro in bitcoin (moneta virtuale, dall'attuale valore di circa 217 euro, che non viene distribuita da alcuna autorità centrale tale da poter tracciare la transazione in quanto le operazioni sono gestite collettivamente da network attraverso dei siti cosiddetti exchanger che rilasciano moneta virtuale incrementando moneta proveniente da carte di credito o altri strumenti elettronici di pagamento) a fronte del quale ricevere, sempre via email, un programma per la decriptazione dei dati.

È importante non cedere al ricatto anche perché non è certo che dopo aver effettuato il pagamento venga restituito l'utilizzo dei file criptati. La migliore arma per difendersi contro questi attacchi ed impedire l'infezione "Cryptorloker" al proprio Pc, oltre che a munirsi di un buon antivirus e fare una copia dei propri file, resta sempre quella di porre la massima

attenzione alle email che si ricevono, specialmente se non attese, evitando di cliccare sul link o di aprire eventuali allegati.

A tal riguardo per avere maggiori informazioni ed assicurare un contatto diretto e continuativo con il cittadino, è possibile fare riferimento anche al commissariato di Ps online, per tutti coloro che frequentano la rete, caratterizzato da innovativi sistemi per poter interagire con l'utente, reperibile all'url: wwwcommissariatodips.it. Il portale è stato integrato di apposita "app" scaricabile gratuitamente dal proprio smartphone e Ipad per consentire di venire incontro alle crescenti richieste di assistenza e di aiuto degli utenti della rete, in tempo reale, e di conoscere sempre di più i rischi e i pericoli derivanti dalla navigazione in rete.