Polizia di Stato

Furto di dati e riscatto in bitcoin, presi con l'operazione "Cryptowash"

Bastava aprire una email apparentemente proveniente da un corriere per le spedizioni o da agenzie governative nazionali, aprire il link o l'allegato, e il gioco era fatto.

Un virus del genere cryptolocker si impadroniva dei dati presenti nella memoria del computer rendendoli accessibili soltanto con un programma per la decriptazione. Il software necessario per questa operazione veniva "offerto" dietro pagamento di un vero e proprio riscatto, che le vittime della truffa erano costrette a pagare.

L'attività dell'organizzazione criminale che aveva architettato il raggiro è stata interrotta dalla Polizia postale di Trieste che al termine dell'operazione "Cryptowash" ha denunciato sette persone con l'accusa di associazione per delinquere finalizzata all'accesso abusivo informatico, estorsione e riciclaggio degli illeciti proventi realizzati. Gli indagati hanno tra i 23 e i 27 anni, tranne un quarantenne che ha un'attività nel settore informatico.

Sottoposto a sequestro preventivo il sito coinbit.it mentre durante le perquisizioni svolte tra le province di Bergamo, Brescia e Padova sono stati sequestrati anche computer, hard disk, tablet, pen drive usb, smartphone, carte di credito e documentazione ritenuta utile alle indagini.

La banda di cybercriminali era da alcuni mesi diventata il terrore del web, e aveva mietuto vittime in tutta Italia tra privati e aziende, colpendo anche tribunali e uffici comunali.

Per riaprire i file criptati, gli utenti erano costretti a pagare un riscatto in bitcoin (moneta elettronica virtuale convertibile in moneta reale) a fronte del quale veniva inviato via email un programma per la decriptazione dei dati. Dai primi riscontri risulta che i criminali abbiano incamerato oltre 277 mila euro di proventi illeciti.

L'indagine della Postale ha avuto una svolta nel marzo scorso, dopo la denuncia presentata dall'amministratore delegato di una società che aveva subito proprio quel genere di ricatto e che aveva pagato per riavere i suoi dati.

Partendo da questo elemento gli investigatori hanno individuato una persona in provincia di Padova, e da questa sono poi arrivati agli altri elementi della banda.

Questi si presentavano come semplici intermediari di coinbit, dichiarandosi estranei alla diffusione del virus, e sui propri siti invitavano le vittime a non pagare il riscatto ma a sporgere denuncia alla Polizia postale.

In realtà erano tutti al corrente della natura illecita dei proventi incamerati dalla società poiché gli specialisti della Postale, oltre alle transazioni effettuate a seguito dei pagamenti, hanno trovato anche centinaia di messaggi che gli indagati si inviavano tramite smartphone.

In questi messaggi si scambiavano consigli sulla diffusione del virus, su come riciclare il denaro, sul comportamento da tenere davanti alle Forze di polizia, e sugli avvocati di fiducia da nominare in caso di bisogno.

Alcuni consigli

E' importante non cedere al ricatto, anche perché non è certo che dopo il pagamento vengano restituiti i file criptati!

Tenere sempre aggiornato il software del proprio computer, munirsi di un buon antivirus, fare sempre un backup, ovvero una copia dei propri file, ma soprattutto fare attenzione alle mail che ci arrivano, specialmente se non attese, evitando di cliccare sui link o di aprire gli allegati, sono i consigli più importanti da seguire per impedire l'infezione del Cryptolocker.

Per maggiori informazioni si può fare riferimento anche al Commissariato di P.S. On-line, caratterizzato da innovativi sistemi di interattività con l'utente: www.commissariatodips.it.

Il portale è stato appena integrato con apposita "app" scaricabile gratuitamente dal proprio smartphone o dall'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 il mondo del web, i suoi rischi e le sue opportunità.

08/07/2015