Internet: la Postale diffonde un anti-malware contro "GandCrab"

Il GandCrab è uno degli attacchi malware più aggressivi degli ultimi mesi, che ha contagiato quasi mezzo milione di vittime da quando è stato rilevato per la prima volta nel gennaio 2018.

La Polizia postale ha collaborato con Europol ed omologhe Polizie estere europee per sviluppare un nuovo strumento di decrittografia che è stato pubblicato gratuitamente su www.nomoreransom.org – il portale di Europol dedicato alla materia. Questo strumento consente di recuperare i file che sono oggetto di infezione del ransonware GandCrab.

Una volta che il ransomware rileva il computer di una vittima e crittografa i suoi file, lo sviluppatore richiede un riscatto che va da 300 a 6 mila dollari. Il riscatto deve essere pagato tramite valute virtuali note per rendere difficilmente tracciabili le transazioni online, come Dash e Bitcoin.

Quanto messo a punto dalle Polizie postali europee rappresenta uno strumento completo di decrittografia in quanto funziona per tutte le versioni esistenti del malware, indipendentemente dalla posizione geografica della vittima.

La rapida diffusione della nuova versione del malware è dovuta al fatto che offre, sul darknet, a cybercriminali anche con poca o nessuna esperienza tecnica, una cassetta degli attrezzi informatici per lanciare attacchi di malware facili e veloci.

La migliore strategia contro le campagne ransomware rimane comunque quella di attivare corrette procedure preventive. La Polizia postale consiglia alle vittime di ransomware di non pagare il riscatto richiesto, in quanto, oltre a finanziare forme di criminalità informatica, nessuno può garantire l´effettiva decrittazione dei file cifrati.

26/10/2018