Certificato n° ER-0075/2016

BORGOSESIA (VC)
Tel. 0163 25327
idsborgo@ids-web.it

TORINO
Tel. 335 7583757
idsturin@ids-web.it

Informatica
Data
System
www.ids-web.it

A tutti i clienti IDS

OGGETTO : Il problema Cryptolocker; cosa fare per difendersi

Ormai da alcuni mesi siamo di fronte ad una nuova minaccia informatica che può provocare notevoli danni e bloccare i Sistemi informatici delle aziende, denominata Cryptolocker.

Riteniamo pertanto utile fornirVi alcune informazioni e possibili suggerimenti sull'argomento.

Cos'è Cryptolocker

I malware della famiglia Cryptolocker non sono "virus" e pertanto non vengono intercettati dai software antivirus, ma sono un complesso sistema definito "Ramsonware" che utilizza strumenti e architetture legali per fare cose illegali.
Ramsonware è la generica etichetta con cui si classificano i programmi maligni che, utilizzando tecniche di cifratura dei file, rendono inutilizzabili documenti, archivi, immagini e qualunque altro contenuto sia memorizzato sul disco, o sulle cartelle condivise, del PC su cui è stato attivato il Ramsonware.
L'operazione criminale è il preludio di una manovra estorsiva che si realizza con il rilascio di una parola chiave in grado di decriptare i file intaccati, a fronte del pagamento di una determinata somma: "ramson", infatti, è il termine anglofono che identifica il riscatto.
Molto spesso, anche a fronte del pagamento del riscatto richiesto, non si ottiene un completo ripristino dei file crittografati.
A cadere in una simile dolorosissima trappola sono stati molti utenti e parecchie aziende hanno visto compromesso il vitale patrimonio informativo, subendo considerevoli danni.

Come si prende Cryptolocker

Solitamente Cryptolocker è contenuto in un messaggio e-mail ricevuto sulla propria casella di posta elettronica. Il messaggio e-mail contiene un allegato oppure un link; aprendo l'allegato o cliccando sul link viene attivato il programma Ramsonware che provvedere a criptare i file contenuti sul disco del PC e sulle cartelle condivise dal PC stesso.
Dal quel momento i file criptati sono inutilizzabili ed il loro contenuto viene irrimediabilmente perso.

BORGOSESIA (VC)
Tel. 0163 25327
idsborgo@ids-web.it

TORINO
Tel. 335 7583757
idsturin@ids-web.it

Informatica Data System
www.ids-web.it

Come si ripristina un PC infetto

Premettendo che non esiste una soluzione al ripristino dei file criptati e che quindi essi verranno persi, molto spesso per eliminare il Ramsonware da una macchina infetta si rende necessario formattare il PC, con la conseguente perdita totale dei dati e delle applicazioni residenti sulla macchina.
In questa situazione il ripristino delle funzionalità della macchina può essere molto lungo e difficoltoso e non sempre garantito al 100%.
I costi dell'operazione di ripristino possono essere pertanto molto elevati anche in considerazione del fatto che si subiranno fermi prolungati della macchina o delle macchine infettate.

Come ci si difende da Cryptolocker

Va detto subito che alla data non ci sono soluzioni tecnologiche disponibili sul mercato in grado di risolvere alla radice il problema.
Come prima cosa è necessario pertanto che le aziende ed i loro utenti prestino molta attenzione durante l'apertura dei messaggi di posta elettronica.
L'apertura della mail di per se non fa scattare Cryptolocker che si attiva solo nel momento in cui apro l'allegato o clicco sul link presente all'interno del testo della mail.
Alcuni controlli "visivi", che possono essere fatti sulla mail sono :

1. Assicurarsi che il nome e l'indirizzo mail del mittente sia corretto e conosciuto, ovvero provenga effettivamente dal dominio di posta dell'organizzazione di cui il mittente dichiara di far parte.
2. Verificare che il testo della mail sia scritto con un linguaggio corretto, con i verbi coniugati in maniera corretta e con una costruzione delle frasi corretta.
3. Verificare che il testo della mail riporti dati corretti e coerenti con la propria attività (loghi, indirizzi, P.IVA, riferimenti ad ordini o ad offerte, ecc)
4. Sono molto pericolose tutte quelle mail che sembrano provenire da mittenti istituzionali (Istituti Bancari, Agenzia delle Entrate, Poste, gestori telefonici, gestori di energia elettrica, ecc) che richiedono la verifica di alcuni dati e presentano un link per la verifica di tali dati.
5. Sono altrettanto pericolosi messaggi provenienti da ipotetici clienti o fornitori non conosciuti e che portano in allegato un potenziale ordine o offerta.

Sulla base della nostra esperienza sul campo l'unica difesa reale che riteniamo possibile per le aziende è quella di dotarsi di un Sistema di backup efficiente, con software in grado di eseguire automaticamente il salvataggio giornaliero delle immagini disco dei PC e dei server aziendali su apparecchiature storage di rete.
Un sistema di backup efficiente con le caratteristiche sopra indicate garantisce, in caso di infezioni da Ramsonware, il completo ripristino dell'apparecchiatura infetta all'ultimo salvataggio in tempi molto brevi, dell'ordine di 1-2 ore.

Qualora foste interessati ad approfondire l'argomento il nostro personale tecnico e commerciale è a Vostra completa disposizione.

Certi di avere fatto cosa gradita, cogliamo l'occasione per porgere cordiali saluti.