Nuovi virus informatici

Una nuova minaccia sta intaccando la sicurezza dei PC e dei dispositivi mobile di mezzo pianeta e, come spesso accade, la diffusione avviene via email o pagine WEB, attraverso un virus di tipo Ramsonware (cioè con richiesta di riscatto) denominato Cryptolocker o CTB Locker.

CryptoLocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da istituzioni legittime. Nelle ultime settimane, ad esempio, circola un' e-mail contraffatta che usa nomi, logo, disclaimer di SDA Express Courrier. Si tratta di un'azione fraudolenta assolutamente non autorizzata da SDA. La stessa cosa potrebbe accadere con e-mail che usano fraudolentemente nomi e loghi di famosi istituti bancari.

All'interno delle suddette mail è presente un link di rimando ad un sito internet malevolo oppure un allegato (che sembra un file di tipo PDF, ma è un programma). Entrambe, se cliccati dall'Operatore, scaricano il CryptoLocker ed iniziano a cifrare (criptare) i files del disco fisso, i dischi di rete mappati sul pc e le unità USB inserite. Viene poi richiesto un "riscatto" per poter avere la chiave per decifrare i dati infettati.

La richiesta di pagamento per sbloccare il computer, è in Bitcoin, la moneta virtuale non tracciabile, ma - è bene evidenziare - che il pagamento non da la certezza che i dati siano resi fruibili ed il consiglio (anche da parte delle Polizie Postali) è di non cedere al ricatto.

Quindi: I files corrotti non sono recuperabili. La sola possibilità è il ripristino da un backup.

Esempio di videata con richiesta di "riscatto" a seguito di infezione di un CryptoLocker.

Valenza Ufficio Servizi Snc
Via Noce 5/B
15048 Valenza (AL)
Tel. +39 0131 955576
Fax +39 0131 942803
e-mail info@valenzaufficio.it
PEC: info@pec.valenzaufficio.it

Proteggersi dai virus, tutelare il proprio lavoro.

Come accennato, la diffusione dei virus avviene quasi esclusivamente mediante email o pagine WEB infette.

Partendo da una analisi dello strumento di diffusione (il Web), abbiamo notato che gli attacchi più dannosi si sono verificati dove venivano utilizzati servizi di e-mail senza protezione antivirus a monte (ad es. alcune e-mail gratuite o fornite in dotazione a linee ADSL) o senza protezione antivirus locale sui PC. Abbiamo anche appurato che le infezioni, quasi sempre, sono riconducibili all'azione di un operatore che ha aperto allegati di e-mail truffaldine oppure ha cliccato su link a siti web virali (cadendo inavvertitamente nella "trappola" dei pirati informatici). Inoltre, quando si è verificata l'esigenza di recuperare i dati dalle copie di backup perché i dati sui PC erano stati criptati o pesantemente danneggiati, nel 50% dei casi ci siamo trovati con copie di sicurezzza non aggiornate o addirittura colpite a loro volta dallo stesso virus (e quindi inutilizzabili).

Premettendo che non esiste un sistema di protezione che dia la sicurezza totale contro attacchi di virus e/o hackers, Valenza Ufficio Servizi consiglia una serie di strumenti e di "comportamenti" da adottare che portano il sistema antivirus ad un buon livello di efficacia:

- Utilizzare e-mail professionali (magari legate al Vs dominio Internet) protette da antivirus alla fonte.
- Fornirsi di un software professionale di protezione dai virus e monitorare eventuali segnalazioni o rilevamenti.
- Controllare sempre chi è il mittente del messaggio di posta elettronica. Se l'e-mail proviene da una banca o altro ente ma si hanno dubbi verificare sempre con la banca stessa la legittimità del messaggio.
- Verificare se nel contenuto del messaggio ci sono evidenti errori (anche grammaticali) o discrepanze.
- Evitare di fare clic su collegamenti o aprire allegati se sospetti.
- Non usare programmi di file-sharing (Emule, uTorrent, Lime, etc) per scaricare film, libri o musica. Oltre a violare (sovente) i diritti d'autore, non si sa che cosa si sta scaricando finchè non si è copiato il file nel proprio PC. Se nel file (spesso zippato) si nasconde un virus, è altissimo il rischio infezione.
- Fare sempre il backup dei dati importanti e verificare il buon esito delle copie.
- Scaricate regolarmente i «security patches» di Windows e dei programmi che utilizzate (modifiche per incrementare la sicurezza dei software).

Valenza Ufficio Servizi Snc
Via Noce 5/B
15048 Valenza (AL)

Tel. +39 0131 955576
Fax +39 0131 942803
e-mail info@valenzaufficio.it
PEC: info@pec.valenzaufficio.it

Il progetto “Lan & Endpoint security” di Valenza Ufficio (Sicurezza a 360 gradi per utenti e dati)

La nostra proposta per proteggere i dispositivi dei Clienti analizza ed affronta ogni punto sopra elencato puntando sulla sinergia tra gli operatori del Cliente ed il nostro personale tecnico.

Sarà cura del Cliente (e dei propri operatori) adottare i comportamenti idonei a prevenire le infezioni, sarà cura di Valenza Ufficio cercare, scegliere e proporre gli strumenti ed i servizi adatti a proteggere i PC, addestrare al meglio gli operatori per evitare le trappole informatiche e monitorare a distanza (da remoto) i punti critici delle infrastrutture informatiche da proteggere.

Il servizio Lan & Endpoint Security è composto da:

- Fornitura di email e domini internet professionali (Valenza Ufficio è partner professionale dei provider Register.it ed Aruba)
- Programma antivirus Sophos con controllo da remoto dei PC installati (due volte al giorno controlliamo eventuali minacce ed attacchi di virus sui Vs PC mediante un sistema di monitoraggio a distanza). Se il sistema Sophos rileva un virus su un Vs PC, viene avvisato il vostro operatore ed il nostro servizio tecnico, prima di procedere alla disinfestazione della minaccia.
- Blocco (da parte del sistema Sophos) di accessi a siti non considerati sicuri e comunque inopportuni (tipo siti pornografici), blocco all’utilizzo di programmi di file sharing (es. Emule, uTorrent, etc) per evitare di scaricare files infetti, avviso e monitoraggio sull’utilizzo dei social media (facebook, twitter, linkedyn, etc.).
- Mini corsi di addestramento ai Vs. operatori sui pericoli informatici e sui comportamenti da tenere per prevenire infezioni da virus informatici.
- Backup automatizzati giornalieri (5 giorni in linea) su dispositivi protetti da password (e quindi ad accesso controllato), con inoltro automatico di una email al nostro reparto di assistenza che indichi lo stato del backup (andato a buon fine, con errori, non avvenuto). In alternativa, se la mole di dati lo permette, utilizzo di Aruba Backup, servizio in cluod per tenere le copie di sicurezza al sicuro dai cryptolocker.
- Controllo annuale dei Vs sistemi informatici in occasione del rinnovo delle Misure di Sicurezza dei Dati Personali del GDPR (Regolamento Europeo N. 679/2016).

Per informazioni ed approfondimenti, contattate il nostro Servizio di Assistenza Clienti al numero 0131 955576

Valenza Ufficio Servizi Snc
Via Noce 5/B
15048 Valenza (AL)

Tel. +39 0131 955576
Fax +39 0131 942803
e-mail info@valenzaufficio.it
PEC: info@pec.valenzaufficio.it