Team Memores Computer – Informazioni tecniche sulla sicurezza informatica

◀◀ ATTENZIONE: I VOSTRI DATI POTREBBERO ESSERE A RISCHIO ▶▶

Segnaliamo che con sempre maggior frequenza si registrano infezioni da un virus molto dannoso che cifra tutti i file del computer rendendoli illeggibili: CryptoLocker

Come si viene colpiti da questo virus?

Molto spesso l'infezione virale da ***CryptoLocker*** si propaga sotto forma di email provenienti da mittenti in genere sconosciuti a chi le riceve, ma anche a volte "spacciandosi" come comunicati di importanti aziende, enti governativi o forze dell'ordine, e sempre contenenti **allegati infetti** con estensioni di vario tipo (*.CAB .ZIP, etc)* o con **invito a cliccare su collegamenti** (link) a siti web (infetti) per "ulteriori informazioni". Gli argomenti delle mail infettanti possono essere i piu' svariati: *bollette da pagare, spedizioni in corso, atti giudiziari, comunicazioni bancarie, etc.*
L'infezione puo' essere contratta anche visitando direttamente siti web precedentemente infettati/danneggiati o comunque appositamente predisposti malevolmente per il contagio.

Immediatamente dopo l'infezione (che consiste nella penetrazione nella memoria del computer) il virus procede alla scansione del sistema e attiva una procedura di "cifratura" dei file con una password molto complessa e pressoche' inviolabile, rendendoli quindi inutilizzabili.
Comparira' quindi una schermata di notifica segnalando che i dati sono stati criptati e che, per poterli recuperare, e' necessario richiedere la speciale password di decodifica procedendo al pagamento di un determinato importo, normalmente richiesto in *BitCoin*, ossia in una criptovaluta elettronica di nuova generazione utilizzando la quale i beneficiari della eventuale transazione di pagamento non saranno rintracciabili.

Questo virus è in grado di colpire la maggior parte delle versioni di Windows desktop e server, inclusi i sistemi Windows XP e Windows Server 2003 (…entrambi particolarmente a rischio!), Windows Vista, Windows 7 e Windows 8.x.

Cosa fare per proteggersi?

- *Aggiornare o sostituire quanto prima nel proprio sistema informativo eventuali macchine dotate di sistema operativo non piu' supportato dagli **aggiornamenti di sicurezza** rilasciati periodicamente da Microsoft (**Windows XP** e **Windows Server 2003**).*
- *Verificare di disporre nei computer di un **buon software antivirus** correttamente installato, configurato e sempre costantemente aggiornato.*
- *Dotarsi di un sistema **Firewall (con APT Blocker)** di nuova generazione, predisposto per intercettare le nuove "minacce evolute persistenti" (Advanced Persistent Threats o APT) alla cui famiglia appartiene anche il pericoloso virus CryptoLocker*
- *Fare molta attenzione alla gestione del contenuto delle **email dai contenuti "ambigui"**, specialmente contenenti allegati o riferimenti/collegamenti a siti esterni.*
- *Evitare di accedere a **siti "sospetti"** o potenzialmente fonte di infezione (...magari segnalati da banner o da inserti pubblicitari particolarmente allettanti).*
- *Effettuare regolarmente (quotidianamente) le **copie di salvataggio** di TUTTI I DATI IMPORTANTI del sistema.*
- *Conservare almeno una **copia (mensile o bi-settimanale) di salvataggio archiviata off-line** (non accessibile sempre e direttamente in rete LAN aziendale), da cui recuperare eventuali dati precedenti il "danno da virus" qualora questo si renda evidente con tempistiche successive alla periodicita' dei normali salvataggi.*

E quando si viene comunque infettati?

Contattare immediatamente un esperto di sicurezza informatica per l'individuazione della strategia ottimale per il recupero dei dati e il ripristino delle difese antivirus del sistema.

Team Memores Computer **spa e' Gold Partner di Kaspersky Lab (tecnologia leader a livello mondiale per la sicurezza e la protezione da *virus* e *malware*) ed e' Rivenditore Certificato di WatchGuard Technologies, azienda specializzata nella produzione di dispositivi Firewall di nuova generazione con *APT Blocker*, predisposti per intercettare le cosiddette "minacce evolute persistenti" tra le quali anche la famiglia di *malware* a cui appartiene, in alcune sue versioni/"*mutazioni*", il pericoloso virus *CryptoLocker* .**

WatchGuard KASPERSKY

Lo Staff Tecnico Certificato di Team Memores Computer e' disponibile a supportarVi e a consigliarVi in tutte le situazioni critiche sottintese ad infezioni virali (compreso *CryptoLocker*) ed a compromissione dei dati.

◀◀ PROTEGGETE I VOSTRI DATI ▶▶

Non esitate a richiederci una analisi preventiva gratuita della Vostra sicurezza informatica!
Contattateci al numero: *0523 576922* e/o visitate il nostro sito: *www.teammemores.it*