Speedcrypt Primi Passi: breve guida in italiano.

Introduzione:

Questa breve guida è il prosieguo di quella pubblicata nel sito e spiega le procedure da compiere per effettuare operazioni relative ai processi di cifratura e decifratura delle liste di file. Si presume che, leggendo questa esposizione, l'utilizzatore del *Progetto Speedcrypt* abbia già letto ed ottemperato ai suggerimenti proposti e caldeggiati negli assunti della breve guida online.

Quanto segue indica quella che dovrebbe essere la miglior strategia per un proficuo utilizzo del progetto. In merito è consigliabile effettuare i test propedeutici relativi a crittografia, derivazioni HASH, compressione e cancellazione dei file matrice. *Ciò consente di adattare Speedcrypt al proprio sistema ed ottenere prestazioni di elevato profilo, oltre che prendere confidenza col progetto e padroneggiare le sue funzioni nel miglior modo possibile*!

Lo schema di cifratura

Speedcrypt predispone, per default, uno schema di cifratura, così come abbiamo visto nella prima parte della breve guida pubblicata sul sito. Personalmente lavoro molto con lo schema seguente:

- *PGP: il motore di cifratura dei file.*
- *Argon2id: la funzione di HASH con la quale verrà derivata la Master Key.*
- *Zip: l'algoritmo di compressione. Il motore PGP lo utilizza per default.*
- *DoD 7 Passes: l'algoritmo di cancellazione dei file matrice.*

Questo per quanto concerne lo schema base modificabile e memorizzabile in base alle proprie esigenze e quelle del sistema *dove Speedcrypt* viene utilizzato. Naturalmente allo schema base vengono addizionate altre funzioni che rendono il processo di cifratura completo e performante:

- *Fortuna: il generatore di numeri pseudo casuali che diverranno il SALT.*
- *BLAKE 256: la funzione di derivazione applicata al SALT*
- *ChaCha20-Poly1305: Il motore di cifratura del SALT*

Quando lavoro con il motore *PGP* predispongo il percorso della generazione delle chiavi *Pubblica* e *Privata* in modo che vengano create direttamente in una chiavetta *USB* da riporre poi in un luogo sicuro noto solamente al sottoscritto. Suddetta chiavetta verrà impegnata nei processi di cifratura decifratura delle liste di file. Stessa tecnica anche con gli altri motori di cifratura: memorizzo sempre sempre le *Master Key* dentro una chiavetta *USB*.

Faccio sempre in modo che non rimanga traccia alcuna negli HD collegati al sistema e quando cancello le chiavi che non sono più utilizzabili lo faccio con SecureDel, preferibilmente ricorrendo all'algoritmo Gutman 35 Passes. Tendenzialmente predispongo dalle due alle tre chiavette che assolvono solo ed esclusivamente al compito di memorizzare le Master Key, non contengono nessun'altro tipo di informazione o dati. Secondo la strategia del momento, ad ogni supporto *USB* è assegnato un compito specifico che può variare in base al motore di cifratura utilizzato all'incombenza e ai dati da cifrare. Gli accorgimenti sopra descritti consentono di porre al sicuro i propri dati, in modo particolare quelli sensibili. *Se potete, non lasciate alcunché nei vostri*

HD, soprattutto se lavorate con Windows, e cifrate quanto più possibile i dati che, giocoforza, debbono rimanere nel sistema!

Master Key: modalità di inserimento

Speedcrypt offre ai suoi utilizzatori due distinte modalità di inserimento per quanto riguarda le *Master Key*, entrambe progettate per offrire il massimo della sicurezza:

- *Immissione per trascinamento col mouse.*
- *Immissione per digitazione da tastiera.*

In entrambe le modalità di inserimento, *Speedcrypt* tenta comunque di creare, partendo dalla stringa inserita dall'utente, delle *Master Key* quanto più complicate possibile, ricorrendo alla *tecnica del riempimento*, come spiegato in questa pagina online della guida. Cionondimeno è molto importante che le chiavi inserite siano quanto più complicate possibile. *Una buona stringa di base innalzerà sicuramente il livello di protezione dell'intero processo!*

La scelta della modalità di inserimento è dettata prevalentemente da una serie di fattori legati all'ambiente nel quale si opera:

- *Tipologia dei dati da porre sotto tutela, quindi il grado di sensibilità.*
- *Sicurezza del proprio sistema, la presenza o meno di programmi dannosi di tipo Keylogger o altri software spia che si ritiene possano aver infettato il PC.*
- *Capacità mnemonica nel rammentare le stringhe inserite.*
- *L'ambiente di lavoro nel quale si opera col PC, che potrebbe essere pubblico o privato.*
- *La postazione di lavoro, autonoma oppure un terminale connesso ad una rete locale.*

Esistono altre condizioni, ma per quanto serve a noi, quelle citate sono più che sufficienti. Ed è in base a ciò che si dovrà effettuare la scelta. Vediamo adesso in dettaglio le caratteristiche di entrambe le modalità di inserimento, in modo tale che l'utente possa instradarsi nel giusto percorso.

Immissione per trascinamento col mouse

Questa modalità di inserimento delle *Master Key* non teme i *Keylogger* e non necessita di alcuno sforzo mnemonico per rammentare i caratteri che formano la stringa. Infatti *Speedcrypt* considera come una *Master Key* nomi dei file, cartelle e sottocartelle. Quanto più sarà esteso il percorso per raggiungere il nominativo di un file o di una cartella, tanto più sarà complicata e robusta la *password*. *Potete fare questa considerazione: i vostri HD sono dei potenziali serbatoi di password, ognuna delle quali potrebbe trovarsi in milioni di posizioni dentro le quali sono composte cartelle, sottocartelle e file.*

Un solo requisito è richiesto nel caso specifico: rammentare il percorso col quale è stata generata la Master key, il che non dovrebbe essere affatto difficile. Altresì è possibile che la *password* risieda all'interno di una chiavetta *USB* utilizzata esclusivamente per questo scopo: il livello di sicurezza risulterebbe a questo punto molto più elevato. Questo protocollo di immissione è piuttosto rigido e contempla l'assegnazione di una *Master Key* per ogni processo di cifratura, anche se effettuato con lo stesso motore. *Per ovviare a questa norma improntata alla massima sicurezza è sufficiente predisporre una lista che contempla tutti i file che si vogliono cifrare in modo che ciò avvenga dentro un singolo processo.*

Personalmente utilizzo moltissimo questa modalità, ho predisposto dei percorsi all'interno delle solite chiavette *USB* che utilizzo quando debbo sottoporre a processo di cifratura i dati che ritengo essere ad elevato grado di sensibilità. Ad ogni modo, se si dovesse utilizzare come *Master Key* una delle tantissime sottocartelle presenti all'interno di un disco rigido, per risalire al percorso giusto, un malintenzionato dovrebbe effettuare la derivazione HASH percorso per percorso. Pensate possa essere un'impresa fattibile?

Immissione per digitazione da tastiera

Questo protocollo è suscettibile agli attacchi dei software spia tipo *Keylogger*, infatti tutto ciò che viene digitato da tastiera costituisce un possibile bersaglio da parte di questi software malevoli. *Speedcrypt* anche in questo caso offre il suo aiuto agli utenti, dando modo ai medesimi di sfuggire a questa tipologia di attacco. Lo fa tramite alcune strategie difensive che possiamo così riassumere:

- *Creazione di un Desktop Sicuro con la Modalità Protetta.*
- *Generazione tramite il mouse di una Master Key robusta.*
- *Salvataggio e cifratura della Master Key tramite codice PIN.*

Vediamo adesso in dettaglio come operano le strategie sopra descritte e come utilizzarle in modo che offrano, quanto più possibile, un buon grado di copertura.

Creazione di un Desktop Sicuro con la Modalità Protetta

Dalla versione 1.3 il *Progetto Speedcrypt* introduce la Modalità Protetta, cioè una sorta di *Desktop Sicuro* dentro il quale non possono operare la maggior parte dei *Keylogger* attualmente conosciuti. Per accedere a questa modalità sono necessari i seguenti requisiti:

- *Privilegi di amministratore nella versione con Setup*
- *La presenza nel sistema del .Net Framework 3.5 in entrambe le versioni*

Una volta entrati in questa modalità *Speedcrypt* inibirà alcune sue funzioni per evitare appunto che il digitato possa essere intercettato e carpito dai software spia.

Generazione tramite il mouse di una Master Key robusta

Dopo aver inserito una lista di file da sottoporre a processo di cifratura o decifratura, *Speedcrypt* rende agibile il pannello di inserimento *Master Key* posizionato in altro a sinistra nella finestra principale del progetto. Cliccare alla voce *Insert* e successivamente sul pulsante contrassegnato da due chiavette ed alla voce di fumetto guida "*Password Generator*". Si aprirà a questo punto la finestra preposta alla generazione delle password. Si scelga adesso il metodo di generazione tra *Classico* e *Speedcrypt*, la lunghezza della Master Key, infine si immetta la stringa selezionata tramite il pulsante denominato *Candidate*. *Tutto ciò senza aver digitato un solo tasto!*

Salvataggio e cifratura della Master Key tramite codice PIN

Chiaramente le *password* generate in tal modo non sono facili da rammentare, soprattutto se aventi una determinata lunghezza: ma sono comunque complicate e difficili da scoprire. *Speedcrypt* offre l'opportunità di memorizzare la *Master Key* dentro un file cifrato col motore *AES* avente chiave a *256 Bit*. Per far ciò è necessario inserire un *Codice PIN* facile da rammentare e nel contempo complicato per un malintenzionato. Ci si può aiutare con il generatore di numeri pseudo casuali *Fortuna* e addizionando numeri tramite tastierino. Si faccia in modo di ricorrere alla tastiera il meno possibile, sottraendosi così

all'attacco di eventuali *Keylogger* presenti nel sistema. Il *Codice PIN* può essere di natura alfanumerica, quindi è possibile inserire una commistione di lettere, simboli e numeri.

Il file con dentro la *password* cifrata, per default, verrà denominato *Master Key* ed avrà estensione .msk. Chiaramente sarà possibile generare quante più chiavi si ritiene opportuno, ognuna con un nominativo specifico, richiamabili tramite *Codice PIN*.

Si tenga presente che il protocollo che prevede l'inserimento da tastiera è meno rigido rispetto al trascinamento della *Master Key* e sarà possibile cifrare un numero illimitato di file con la medesima *password*. *Speedcrypt*, anche in questo caso, ordinerà gerarchicamente i file cifrati in base ai processi di cifratura effettuati.

Cifrare e decifrare liste di file

L'inserimento della *Master Key* predispone *Speedcrypt* al processo di cifratura. Durante l'inserimento, come già spiegato, la chiave subisce una trasformazione che renderà la stringa molto più complicata e robusta, ciò avviene tramite un processo di derivazione effettuato con l'algoritmo BLAKE 256 che effettuerà un riempimento e consegnerà la stringa generata alla funzione di HASH selezionata dall'utente. *La derivazione conseguente a questa procedura diverrà la reale Master Key con la quale saranno cifrate e decifrate le liste di file.*

Non resta a questo punto che cliccare alla voce di menu denominata *Encryption* e successivamente alla voce *Encrypt* oppure *Decrypt* list, in base al processo da eseguire. Ciò è fattibile anche tramite il pulsante posizionato nell'apposita barra oppure con il tasto destro del mouse sulla lista dei file.

Una volta eseguita la procedura di cifratura, *Speedcrypt* predisporrà una scaletta gerarchica dei file cifrati, ognuno associato alla *Master Key* utilizzata ed al processo eseguito. In tal modo, per effettuare la procedura di decifratura, sarà sufficiente selezionare i vari gruppi ed inserirli nell'apposita griglia. Questa operazione può avvenire direttamente nel progetto, senza richiamare o trascinare dalla *Shell* di *Windows*.

Se non si ha esigenza di creare dei file di backup relativi ai file cifrati, si tragga in spunta, nella finestra *Settings*, la voce denominata "*Automatically delete Archives after Decryption*" posizionata nella *Tab Page* denominata *Encryption Archives*. Questa operazione consentirà a *Speedcrypt* di rimuovere dal file di configurazione i nominativi dei file cifrati, tenendo presente che verrà comunque creato un file di *backup* che potrà essere utilizzato qualora si abbia necessità.
