VeraCrypt - Crittografia for paranoid people

Author : Fabio Carletti aka Ryuw

Date : 28 Febbraio 2019

La riservatezza, la privacy e l'autenticità dei documenti digitali sono tra i temi più attuali in questo periodo storico. Tra spionaggio governativo e quotidiane violazioni della privacy per scopi commerciali, i tool che ci permettono di difenderci stanno prendendo sempre più piede anche tra gli utenti abituali di internet. Un programma multipiattaforma OpenSource che fa al caso nostro è VeraCrypt, usato per la crittografia "on-the-fly".

Fork del famoso programma (per addetti ai lavori) **TrueCrypt**, VeraCrypt permette di creare dischi virtuali crittografati, o semplici file, contenenti cartelle o molteplici file da inviare nella rete internet. Tra le qualità di questo programma, la possibilità di sfruttare la **crittografia parallela** per sistemi multi-core, così diminuendo moltissimo il tempo necessario per le operazioni di cifratura e decifratura.

La nuova **release 1.23**, uscita ufficialmente a fine 2018, sviluppata in C e C++ da IDRIX, prova che questo progetto è in via di ampliamento, supportato e con un'ottima stima da parte degli utilizzatori, poiché non vi sono backdoor né sistemi che consentano, da parte degli sviluppatori, di recuperare i file crittografati senza l'uso della password-Key.

Nel 2008, negli Stati Uniti, ci fu il caso di Daniel Dantas che, utilizzando TrueCrypt (l'antenato di VeraCrypt prima del fork del progetto) impedì all'FBI di aprire i suoi file, a distanza di oltre un anno dal sequestro dei suoi dati crittografati.

VeraCrypt non ha una versione commerciale: è **pubblico, liberamente scaricabile e utilizzabile** e, per chi è programmatore, è visionabile il codice sorgente.

Con l'avvento di VeraCrypt, rispetto al progetto precedente si sono aggiunti algoritmi di crittografia che rendono più difficile gli attacchi definiti, in gergo tecnico, "bruteforce". Quindi da TrueCrypt a VeraCrypt c'è stato un notevole miglioramento del progetto; tuttavia, nella sicurezza informatica vale sempre il concetto per cui **non basta un prodotto** ma occorrono processi, composti da più fattori, che ci permettano di raggiungere un certo livello di sicurezza.

Programma disponibile anche per i cellulari Android e iOS, VeraCrypt permette di creare

contenitori cifrati che potranno essere gestiti solo da chi conosce la password per accedervi, gestibili nei diversi OS in cui è presente il programma. Per gli scettici e paranoici della crittografia, il sito in cui è visionabile il codice è www.veracrypt.fr/code/, nella cui sezione download si trovano eseguibili per i sistemi operativi di maggiore utilizzo, accompagnati da file PGP (PGP signature).

Per precauzione - potrebbe avvenire che un pacchetto preconfezionato per un sistema non sia regolare - con le PGP signature è possibile verificare l'integrità e l'autenticità di ogni pacchetto di distribuzione di VeraCrypt.

Questo permette di verificare che il pacchetto, anche se scaricato da altre fonti, sia stato creato dal sito di origine e non alterato da un malintenzionato; l'operazione è eseguibile tramite le firme digitali del file. Il team dietro al progetto usa due tipi di firma, una PGP per tutti i sistemi e l'X509, disponibile solo per windows. Le firme PGP presentano dei vantaggi, dato che non dipendono da alcuna autorità di certificazione (che potrebbe essere infiltrata o controllata da un avversario).

Diversi clienti hanno preso l'abitudine di creare una cartella personale con i dati all'interno e crittografarla in una chiavetta usb da portare con sé: in questo modo, anche se si perde la chiavetta, il contenuto rimane segreto e immune da spionaggio industriale. Tra i più famosi **algoritmi che possiamo usare nel programma** vi sono AES, Serpent, Camellia (usato in Giappone) e Kuznyechik (utilizzato in Russia).

Tra gli algoritmi di *hash* troviamo i famosi sha-256, sha-512 e whirlpool, usato da ISO (International Organization for Standardization).

Tra le recenti **integrazioni con windows** c'è la possibilità di creare volumi contenitori semplici, con una procedura guidata e grafiche intuitive, generando un volume nelle risorse del computer, con apposita lettera di unità da utilizzare.

Per gli amanti del terminale, una volta installato, il programma è utilizzabile anche tramite script automatici.

Tra gli usi di VeraCrypt, anche la possibilità - utile in casi estremi - di creare volumi nascosti senza limitazioni, aumentando così la sicurezza informatica. Se qualcuno polemizza sulle tempistiche, lunghe nonostante le ottimizzazioni del calcolo parallelo, esistono in commercio processori che supportano la crittografia AES, con un'accelerazione hardware 6 volte più veloce della procedura software, tramite l'istruzione AES-NI-support, presente sulle CPU recenti più performanti.

Spesso capita di sentirmi chiedere dai clienti, che cerco di sensibilizzare alla sicurezza informatica, se sia meglio avere i dati criptati su cloud o nei NAS, con file-system crittato.

Per rispondere al quesito, solitamente, riporto fatti realmente accaduti: aziende in cui viene rubato il NAS per cercare di vedere documenti e posta elettronica a fini di spionaggio industriale (quindi il cloud è più utile in questi casi, in modo da avere un piano A-B-C). Ancora più utile è

avere un volume criptato nel computer, contenente tutti i file, e il medesimo volume copiato anche in altra sede. VeraCrypt supporta token di sicurezza e smart card a cui è possibile accedere utilizzando il protocollo PKCS#11 (Public-Key Cryptography Standards).

Come ogni strumento, sta alla persona saper scegliere come usarlo: dato che è **gratuito e OpenSource**, servono solo costanza nel suo utilizzo e password difficili da scovare. Per qualsiasi dubbio esistono un forum attivissimo e anche una sezione per le donazioni (da effettuare in cryptovalute come Ethereum, Litecoin e Monero).

Programmi simili a VeraCrypt sono DiskCryptor, Cryptomator, BoxCryptor, LibreCrypt, Axcrypt, FreeOTFE e SecurStick; ci sono anche programmi interni ai sistemi, come BitLocker o FileVault. Reputo VeraCrypt il **top della serie** al momento attuale, per il suo essere multipiattaforma e, soprattutto, sotto licenza d'uso OpenSource, termine tecnico da usare quando i detentori di un software rendono pubblico il codice sorgente, favorendone il libero studio e permettendo, come suggerisce Wikipedia, a programmatori indipendenti di apportarvi modifiche ed estensioni.

Qui sta la sicurezza del progetto: non installiamo una scatola chiusa (software proprietario) in cui potrebbero esserci contenuti indesiderati (come backdoor o trojan), ma un software Free/OpenSource, liberamente visionabile; pertanto, se ci fosse qualcosa di "strano", la comunità che maneggia il codice vedrebbe subito il codice malevolo. Il modello di business dell'OpenSource si basa su donazioni, servizi a pagamento e guadagni provenienti da formazione e didattica.

Concludo con la citazione di Morpheus a Neo nel film Matrix: *"io posso condurti fino alla soglia, ma la porta devi varcarla da solo".*

Articolo a cura di **Fabio Carletti aka Ryuw**