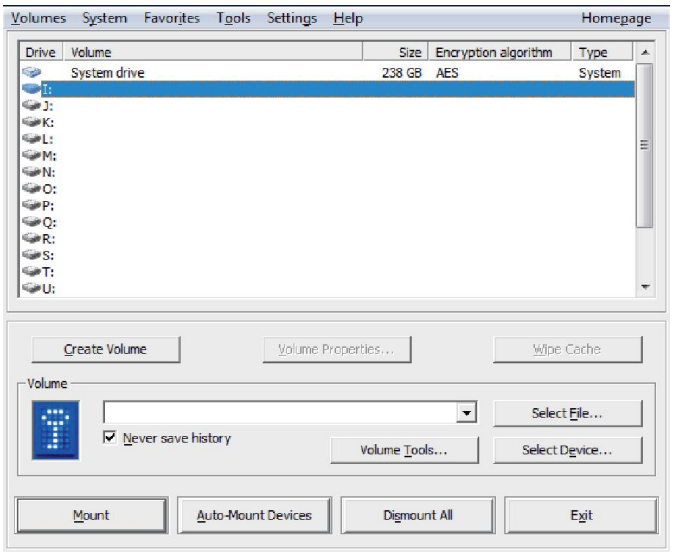
# *TrueCrypt* - šta se dogodilo?

Autor: Aleksandar Todorović

Svako koga malo više zanima privatnost, čuo je za *TrueCrypt* – mali, jednostavan i funkcionalan program preko kojeg korisnici mogu da enkriptuju svoje podatke koristeći trenutno najsigurnije algoritme za enkripciju na tržištu. U nekoliko klikova, korisnici su mogli da enkriptuju datoteke, fascikle, particije, pa čak i čitav disk. Svi podaci su im bili na raspolaganju čim bi ukucali ispravnu šifru i nalazili bi se u privremenom dekriptovanom obliku. Međutim, bez te šifre bilo je nemoguće pristupiti bilo čemu.*Rijndael*, *Serpenth* i *Twofish*, tri najsigurnija algoritma za enkripciju na svijetu, mogla su se koristiti upotrebom samo jedne aplikacije. Za one koji vole dodatnu sigurnost, postojala je i mogućnost kombinovanja tih algoritama. Mogli ste da koristite i sva tri algoritma ukoliko ste stvarno paranoični. *TrueCrypt* se aktivno razvijao čitavu deceniju i zbog svoje dostupnosti na više platformi stekao je više korisnika od bilo kojeg drugog konkurentnog softvera. Njegova licenca je bila „komplikovana" (prim.aut). Ovo nije bio jedan tipičan projekat otvorenog koda. Iako je njegov kod bio javno dostupan, korisnici nisu imali prava da prave svoje verzije (tzv. forkove, eng. *fork*), nisu mogli da učestvuju u njegovom daljem razvijanju, a identiteti njegovih autora nikada nisu bili javno dostupni.



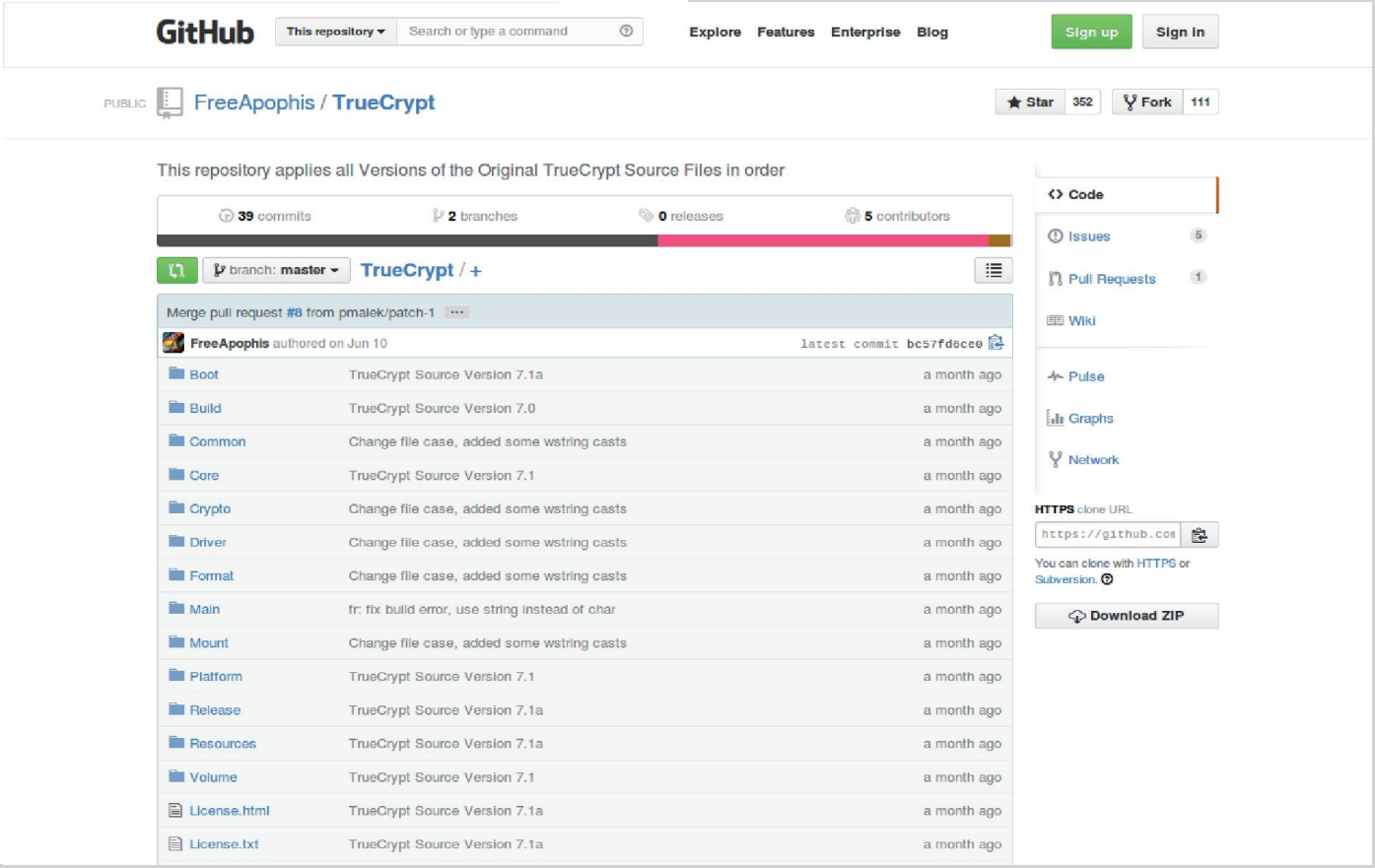

Sledi iznenađenje - na službenoj stranici projekta objavljeno je da je njegova dalja podrška ukinuta. Napisano je da je sa razvojem prekinuto kada je *Windows* ukinuo podršku za *XP* operativni sistem. Na stranici je naglašeno da autori ne vide više potrebu da razvijaju svoj softver jer je bio prvenstveno namijenjen za *Windows*

operativne sisteme i navode kako svi noviji sistemi koje je *Windows* objavio, imaju podržanu enkripciju diska, te da se preporučuje da se podaci enkriptuju alternativnim metodama.

U nastavku teksta se navodi *BitLocker* (integrisani *Windows* alat za enkripciju) kao njegova alternativa, te se detaljno objašnjava njegova upotreba, a na kraju se daje link prema novoj 7.2 verziji *TrueCrypta*, dok su linkovi prema starijoj (7.1 verziji) uklonjeni sa sajta. Nova verzija je zapravo ogoljena stara verzija. Prilikom pokretanja, korisniku se prikazuje poruka o tome da se *TrueCrypt* prestao aktivno razvijati, a iz programa je uklonjena njegova najvažnija funkcionalnost: mogućnost enkripcije. Ova nova verzija služi samo za dekriptovanje podataka, sa ciljem da se korisnici prebace na neki alternativni program.

Kao što je već navedeno, *TrueCrypt* je zbog svoje politike bio daleko od savršenog programa. Zbog svoje licence nije pronašao put niti u jedan softverski centar vodećih *Linux* distribucija. Međutim, radio je posao za koji je bio namijenjen i to vrlo dobro (prim.aut.). Iako za *Linux* postoji nekoliko alternativa, ne postoji niti jedna tako jednostavno odrađena. Alternative su višekomandne, sa pokušajima grafičkih interfejsa koji ne rade dovoljno dobro posao i ne podržavaju sve algoritme koje podržava *TrueCrypt*.

Korisnici su ostavljeni na milost i nemilost slučaju, bez podrške i načina da sigurno zaštite svoje podatke i sve to bez ikakve prethodne najave. Šta sada?



Sada je na red stupila zajednica. Nije lako uništiti program sa interneta ukoliko ga velik broj ljudi aktivno koristi. U roku od nekoliko dana, na internetu su se našli mnogi linkovi prema starijim verzijama. Korisnici mogu preko *hasha* da provjere njihovu autentičnost, a upotreba starije verzije za sobom ne nosi nikakve posljedice, za sada. Međutim, šta kad se nađu propusti?

*TrueCrypt* se smatra vrlo sigurnim. U svojoj istoriji nije imao nikakvih incidenata u smislu da je neko razbio njihovu implementaciju algoritama. To je postalo malo sumnjivo u poslednjih godinu dana, te je zajednica odlučila da preispita softver koji mnogi od nas koriste za zaštitu svojih privatnih podataka. Skupilo se nešto para, okupili su se profesionalci i rad na pregledu tog softvera je počeo. Trajao je jako dugo. Zapravo, nije ni uspio biti završen prije nego što je *TrueCrypt* odlučio da se ugasi. Do tada su eksperti za sigurnost našli neke sitni bagove, ništa revolucionarno što bi u potpunosti pogazilo sigurnost *TrueCrypta*.

Šta sada? Pa, softver u svojoj starijoj verziji može da ostane siguran neko vrijeme. To može da prestane u sljedećih godinu dana, a može i da traje toliko dugo dok ne izađu novi operativni sistemi koji neće biti kompatibilni sa tako zastarjelim softverom. U budućnosti postoji šansa da će neko i uspjeti da razbije njegove algoritme i sve njegove korisnike stavi u opasnost, međutim, uzimajući u obzir da se softver više ne razvija i da sve više osoba preko *IRC*-a i *reddita* traži sigurne alternative, *TrueCrypt* je prestao da bude toliko zanimljiv. Naša preporuka: slobodno ga koristite u sljedećih, recimo, godinu dana, međutim budite svijesni da je potrebno da što prije pređete na neku aplikaciju kojoj vjerujete. Preporučujemo vam da obratite pažnju da bude u aktivnom razvoju (prim.aut.). Izaberite pažljivo svog *TrueCrypt* nasljednika, jer ćete vašem odabiru dati ono što vam je najvrijednije - vaše povjerljive podatke. *TrueCrypt* u 7.1 verziji možete preuzeti sa sljedećeg linka: https://truecrypt.ch