Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Šesta laboratorijska vežba -

6. NTFS alternativni tokovi podataka[1]

NTFS fajl sistem dozvoljava postojanje više tokova podataka pored glavnog toka. Takvi tokovi podataka se nazivaju alternativnim tokovima podataka. Prilikom otvaranja ili pregledanja fajla može se videti samo glavni tok dok su ostali tokovi podataka sakriveni od korisnika. Ovo su neki od primera zamišljene upotrebe alternativnih tokova podataka:

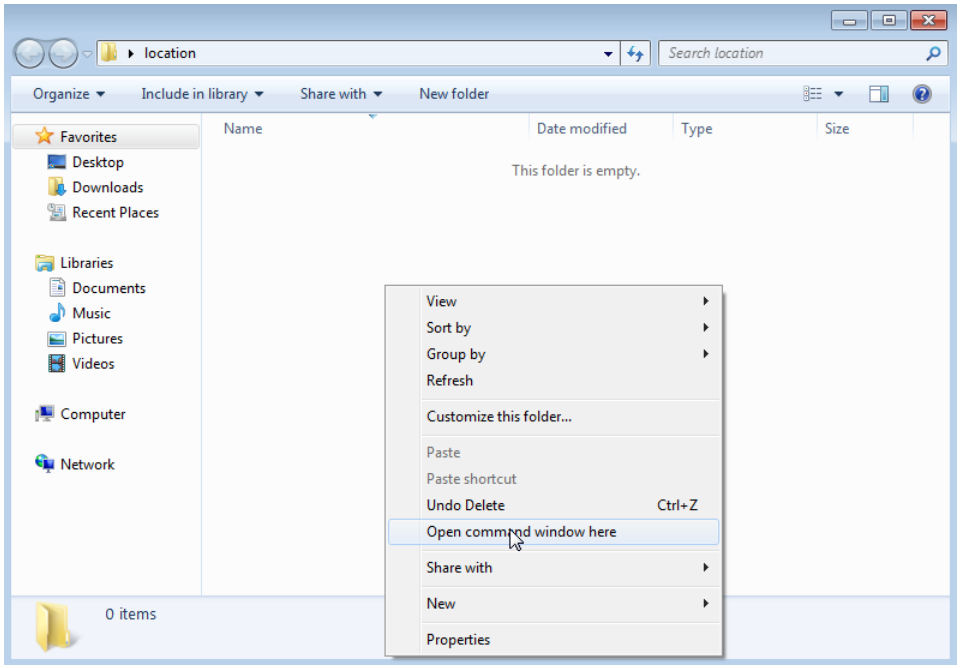
1. **Favoriti unutar Internet Explorer-a**. Pri dodavanju linka nekog veb sajta u svoje favorite tada se kreira .url fajl koji sadrži url i opis tog linka. Međutim, ako veb sajt ima i ikonu(favikon koji se nalazi u tab-u), tada se kreira alternativni tok podataka url fajla sa imenom :favicon:$DATA
2. **Preuzeti fajlovi u Internet Explorer-u**. Prilikom preuzimanja i snimanja fajla sa interneta korišćenjem Internet Explorer-a automatski se dodaje informacija o tome da je taj fajl skinut sa interneta. Naziv toka posataka u ovom slučaju je :ZoneIdentifier: $DATA

Korišćenje alternativnih tokova podataka će ovde biti prikazano kao način za sakrivanje podataka na vidnom mestu, bez ikakve enkripcije i zaštite jer bez posebnog programa koji će ovde biti upotrebljen ne postoji način da pročitamo alternativne tokove podataka osim ako im znamo tačno ime.

Ova laboratorijska vežba se radi na Windows 7 virtuelnoj mašini (VM2). Potrebno je povezati se na tu mašinu putem Remote Desktop-a. U novijim verzijama Windows operativnog sistema postoje integrisani alati za čitanje NTFS tokova podataka o kojima možete pročitati na sledećem linku. Još jedan zanimljiv članak koji detaljnije obrađuje ovu temu nalazi se na ovom linku.

1. Kreirati folder sa imenom location na desktopu i otvoriti ga. Unutar tog foldera pritisnuti desni klik dok držite Shift. Kliknuti na open command window here. Alternativno otvoriti PowerShell i pozicionirati se u ovaj folder.

[1] Nastavnici na predmetu Zaštita računarskih sistema i mreža se zahvaljuju studentu Luki Mrdaku za pripremu scenarija ovu laboratorijsku vežbu



2. Potrebno je kreirati normalan tekstualni fajl koji sadrži neku poruku. Komanda za to je `echo "moja poruka" > file1.txt`

3. Otvaranje fajla za čitanje može se izvršiti komandom **notepad file1.txt**. Proveriti heš vrednost tog fajla komandom `certutil -hashfile file1.txt`. Na kraj ove komade može se dodati **> ime_fajla** da bi se sačuvao izlaz komade unutar fajla sa imenom ime_fajla

4. Dodati tekst koji će predstavljati sadržaj koji bi trebalo da bude sakriven, na primer "vojna tajna" u alternativni tok podataka koji se zove SecretFile.txt i povezati ga sa postojećim fajlom sledećom komandom `echo "vojna tajna" > file1.txt:Secret-File.txt` .

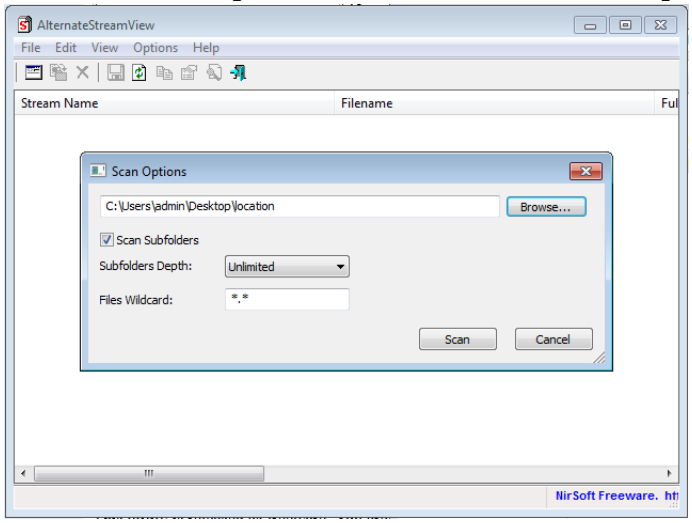
5. Proveriti heš vrednost tog fajla komandom `certutil -hashfile file1.txt`. Uporediti sa prethodno zabeleženom hash vrednošću. Da li se heš vrednost nije promenila? Da li se u File Exploreru veličina fajla promenila? Ovde je umesto teksta od nekoliko bajtova mogla biti dodata i ogromna aplikacija od nekoliko gigabajta koja ne bi i dalje promenila veličinu fajla. Provera da li je heš vrednost odgovarajuća se najčešće koristi za potvrdu da je fajl u svom originalnom obliku i da nije menjan, a to ovde nije slučaj.

6. Sada je potrebno pročitati tajnu poruku koja se nalazi u alternativnom toku podataka komandom `notepad file1.txt:SecretFile.txt`. Da tačan naziv ovog alternativnog toka podataka nije poznat ne bi bilo moguće pročitati ovaj sadržaj bez korišćenja nekih dodatnih alata.

7. Napraviti novi folder sublocation unutar foldera location. Kopirati fajl file1.txt u taj folder i promeniti tekući direktorijum u cmd-u u taj folder koristeći komandu `cd sublocation`. Ponoviti komande za čitanje glavnog i alternativnog toka podataka koristeći notepad. Primetiti da se oba toka podataka kreću zajedno kao jedan fajl.

8. Na VM2 preuzeti program **AlternateStreamView.exe** sa ove lokacije (raspakovati i smestiti u neki pogodan folder). Ovaj program služi za čitanje alternativnih tokova podataka kojima ime nije poznato.

9. Kliknuti na browse i odabrati folder na desktopu gde su kreirani fajlovi koji imaju alternativne tokove podataka. Kliknuti na Scan i pokrenuti skeniranje.



10. Primetiti detektovane tokove podataka. Korišćenjem ovakvih programa mogu se detektovati svi alternativni tokovi podataka, i dobronamerni koji se koriste od strane aplikacija i zlonamerni.