Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Osma laboratorijska vežba -

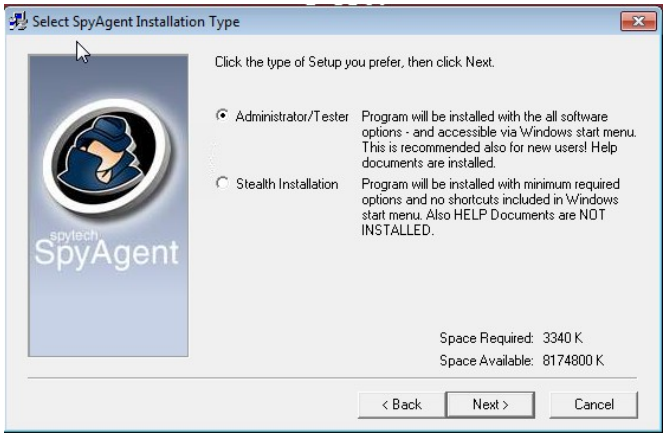
8. Spyware - Spajver[1]

Spajver je maliciozan program koji špijunira i prati radnje korisnika bez njegovog znanja. Postoji nekoliko varijanti spajvera, i to adver (*adware*) koji prati istoriju pretraživača i preuzimanja sa ciljem da plasira reklame za proizvode i usluge, trojanac koji se maskira kao regularan softver, a za to vreme prikuplja podatke, sistem monitori koji prate sve aktivnosti na računaru. Postoje mnogi načini da se računar zarazi spajverom, ali najčešći su prihvatanje pop-up reklame na internetu, preuzimanje softvera iz neproverenih izvora, otvaranje priloga (*attachment*) u mejlovima od nepoznatih pošiljalaca.

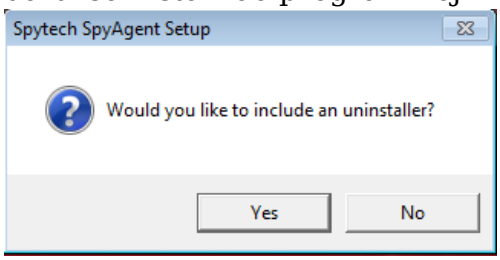
Na sledećem primeru biće ilustrovano koje sve podatke o korisniku jedan spajver može da sakupi. Otvoriti folder gde su otpakovani potrebni alati (Lab 8 tools) i unutar njega otvoriti folder gde se nalazi Spytech SpyAgent. Pokrenuti program Setup, pa kliknuti Next

1. Kliknuti Next sve dok se ne prikaže ovaj prozor. Odabrati Administrator/Tester jer će program biti korišćen za demonstraciju, ali i nekoj pravoj primeni bi bila korišćena druga opcija.

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



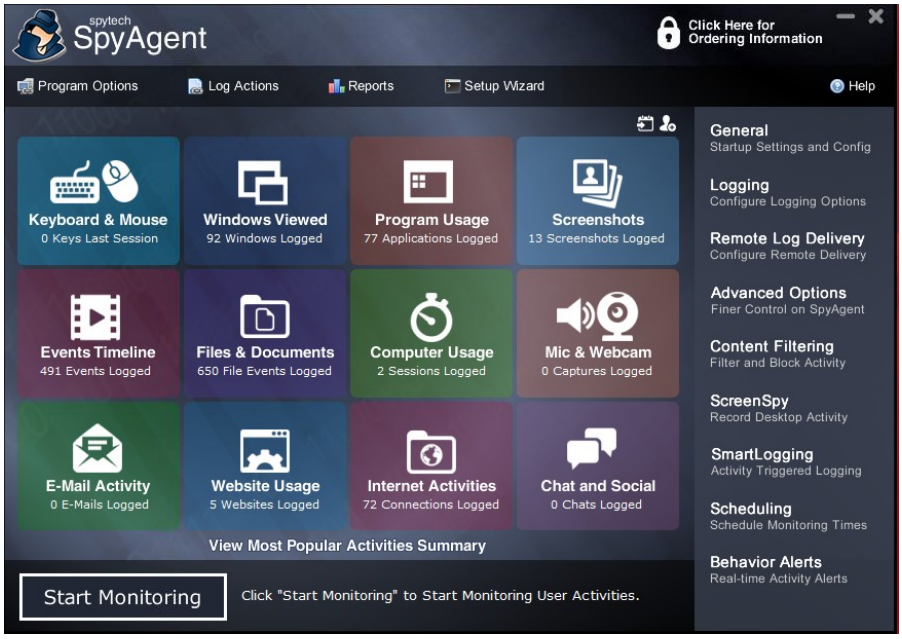
2. Kliknuti Next sve dok se ne pojavi ovaj prozor. Kada se pojavi taj prozor kliknuti “Yes” da bi se instalirao program koji može da izbriše spajver jednostavno sa računara.



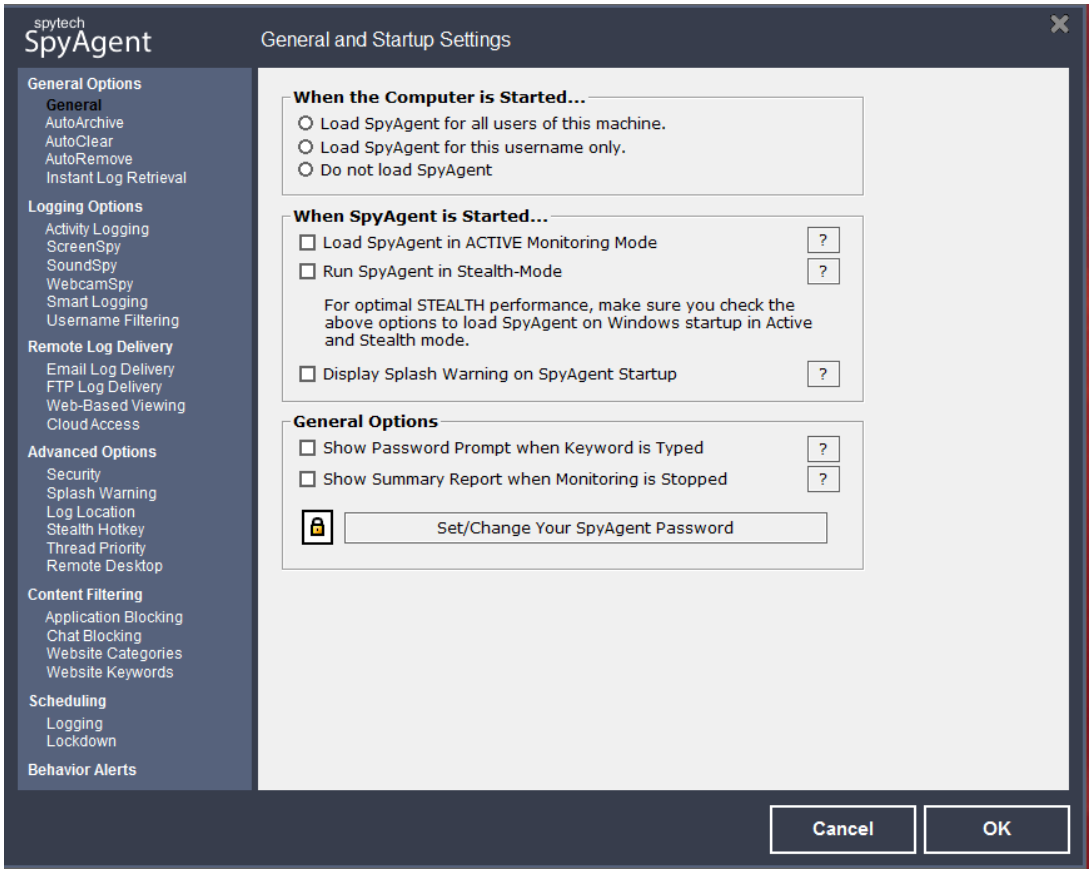
3. Na poslednjem ekranu će se pojaviti opcija da se odmah pokrene ovaj program. Štiklirati tu opciju. Ukoliko je preskočen prethodni korak, instalirani program se nalazi na lokaciji Start->All Programs->Spytech SpyAgent->SpyAgent PC Surveilance.

4. Primetiti početni prozor programa i pročitati tekst sa nekim od mogućih upotreba ovog programa, tu pritisnuti continue

5. Primetiti da je sada otvoren glavni meni programa gde se mogu podešavati događaji i akcije koje će biti praćene na ovom računaru.



6. Kliknuti na Program Options u gornjem levom uglu, pa na Options, pa negde na pop up koji se otvorio. Primetiti da su otvorena podešavanja programa. Ovde je moguće podesiti da li se spajver startuje za sve korisnike na ovom računaru, da li se pokreće u ACTIVE modu gde korisnik vidi da postoji spajver instaliran na njegovom računaru ili u Stealth modu.

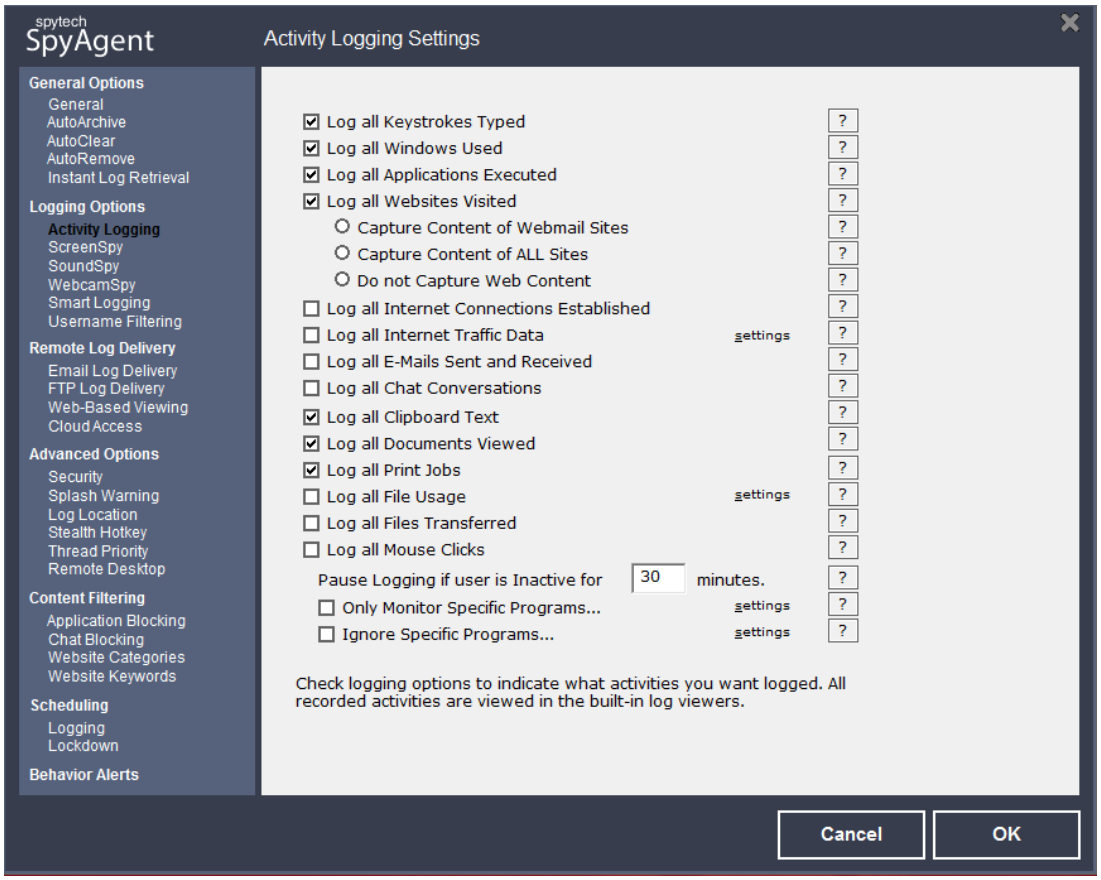


7. Na levoj strani neka od generalnih podešavanja su:

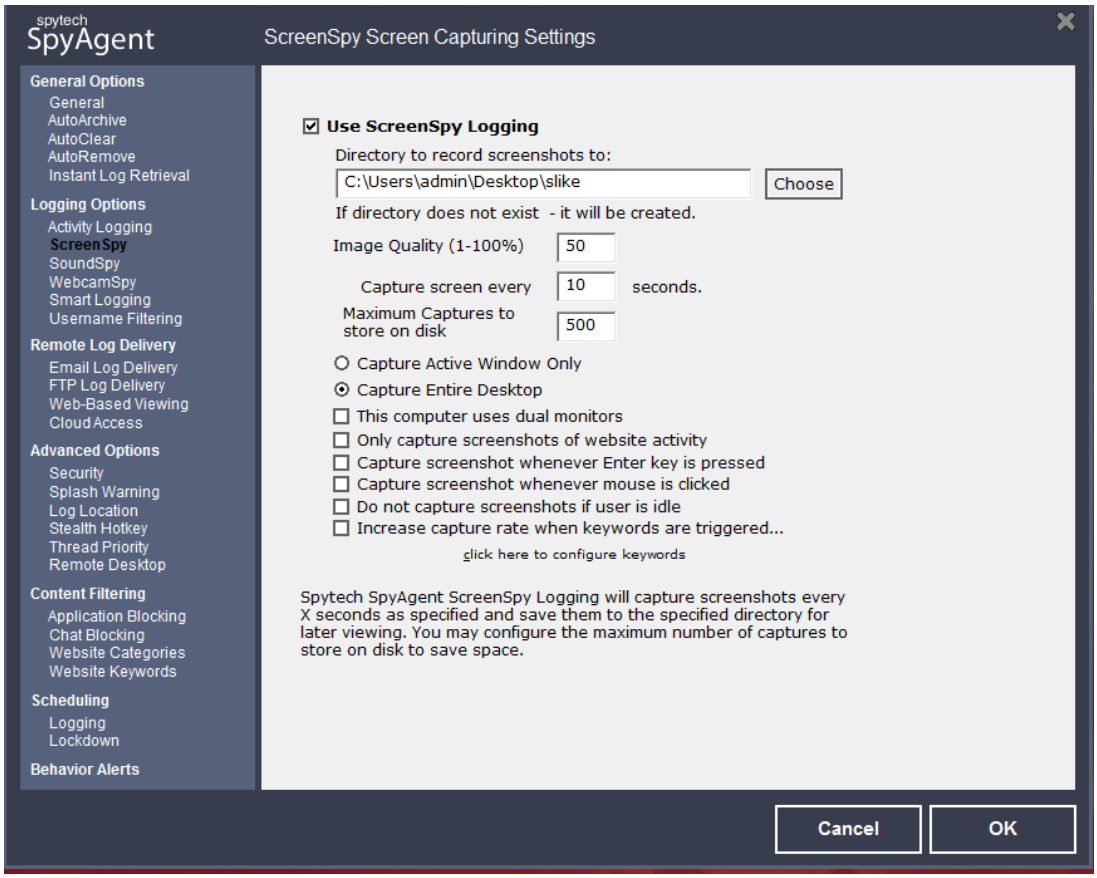
Podešavanje	Objašnjenje
AutoArchive	Da li će se svi logovi SpyAgent-a snimati za kasnije gledanje
AutoClear	Pošto logovi mogu da zauzimaju dosta prostora mogu se brisati nakon određenog vremena, nakon što zauzimaju određenu veličinu, ili za keylogger koliko poslednjih pritisaka tastature da pamti
AutoRemove	Kada će SpyAgent sam sebe da deinstalira
Instant Log Retreival	Podešavanje da kada se neki disk(USB stik ili eksterni hard disk) ubaci u kompjuter da se automatski pokrene kopiranje logova na taj disk

8. Kliknuti na Set/Change Your SpyAgent Password i tu postaviti neku lozinku za SpyLogger (zapamtiti ovu lozinku!), npr. stealth.

9. Nakon toga kliknuti na Logging options i tu podesiti podešavanja kao na slici. Dakle, biće praćeno koje tastere korisnik pritiska, koje prozore koristi, koje aplikacije izvršava, koje sajtove posećuje, šta se nalazi u klipbordu kada kopira fajlove, koje dokumente pregleda i šta štampa.



10. Kliknuti na ScreenSpy na levoj strani prozora i podesiti neku lokaciju gde će se snimati slike. Za potrebe demonstracije najjednostavnije je u nekom novom folderu na desktopu



11. Nakon ovog koraka primetiti da u daljim opcijama postoje snimanje zvuka, slikanje veb kamere i filtriranje korisničkih imena.

12. Sledeća grupa opcija pokriva dostavljanje logova na neki drugi računar. Tu je potrebno primetiti da postoje opcije slanja preko mejla, slanja FTP protokolom, pregledanje logova sa veba ili kroz klaud servise.

13. Naredna grupa opcija predstavlja podešavanja koja omogućavaju dodatno sakrivanje SpyAgent-a, grupa nakon nje su podešavanja filtriranja gde mogu biti ignorisani neki sadržaji sa interneta, neki programi ili neke čet aplikacije i na kraju podešavanje kada u toku dana SpyAgent može da skuplja logove i opcija za slanje upozorenja kada se neka situacija od interesa desi.

14. Kliknuti na Start Monitoring i uneti lozinku. Minimizirati SpyAgent.

15. Sledeći koraci predstavljaju simulaciju rada korisnika na svom računaru gde korisnik nije svestan da na tom računaru postoji instaliran spajver.

16. Otvoriti Notepad, napraviti fajl sa imenom lozinke i napisati nekoliko najuobičajenijih lozinki. Sačuvati taj fajl negde na desktopu. Postoji dosta ljudi koje svoje lozinke čuvaju na ovaj način.

17. Prekopirati prvi pasus sa sledeće lokacije u notepad i sačuvati taj fajl. Primetiti da je ovaj pasus smešna priča, ali isto tako može biti neki CV ili neka druga poslovna tajna koju ne bi smeo bilo ko da pročita.

18. Pritisnuti kombinaciju tastera **Ctrl+Alt+Shift+M**, pa uneti svoju lozinku za SpyAgent. Ovim se otvara SpyAgent za pregled događaja i akcija koje je spajver uhvatio za ovo vreme.

19. Pogledati kartice raznih boja na sredini ekrana i kliknuti na njih i primetiti šta od akcija u prethodnih nekoliko minuta je spajver pokupio. Obratiti posebnu pažnju na programe koji su otvarani i klipbord.

20. Minimizovati spajver. Sledeći koraci predstavljaju nastavak simulacije rada korisnika koji nije svestan postojanja spajvera na svom računaru.

21. Otvoriti sledeći link i kreirati nalog na sledećoj lokaciji (**ova lozinka će se možda sačuvati, koristite neke nasumične podatke**). Ova stranica predstavlja simulaciju stranice za logovanje, ali je isto tako mogla biti stranica za logovanje na studentski mejl, društvene mreže ili eventualno privatni mejl. Tu unesenu lozinku i korisničko ime je spajver uhvatio.

22. Na sledećem linku se nalazi tekst pesme koju je potrebno odštampati. Kada otvorite link pritisnuti **Ctrl+P** i pustite da se odštampa preko Document XPS viewera što simulira štampač. Ova radnja predstavlja simulaciju štampanja ugovora, vlasničkog lista ili bilo kog drugog bitnog dokumenta.

23. Pritisnuti kombinaciju **Ctrl+Alt+Shift+M**, pa uneti lozinku za SpyAgent. Kliknuti na Stop Monitoring.

24. Pogledati kartice raznih boja na sredini ekrana i kliknuti na njih i primetiti šta od akcija u prethodnih nekoliko minuta je spajver pokupio. Posebnu pažnju obratiti na kartice koje odgovaraju poslednje simuliranim akcijama korisnika. Pogledati slike ekrana koje su snimljene.

25. Kliknuti na Reports u gornjem delu programa i izgenerisati neki od izveštaja.

26. Sada je potrebno izbrisati ovaj spajver. Najjednostavnije brisanje ovog spajvera je odlaskom u Control Panel, pa u Programs and Features, pa Spytech SpyAgent pa uninstall, pa yes.