

Til kamp mot SPYWARE

I forbindelse med vår gjennomgang av malware i forrige utgave, introduserte vi spyware, den største komponenten i denne heller tvilsomme programware-gruppen. "90% av all malware er spyware" hevder IT-sikkerhetsselskapet Panda i en fersk pressemelding. Mange av oss sitter med praktiske erfaringer som bekrefter observasjonen.

Nest etter virus og SPAM er *spyware* den største trussel våre IT-systemer er utsatt for. Ifølge et estimat fra IDC blir mellom 67 og 90% av alle PCer med Internett-kontakt infisert av *spyware*. Andre undersøkelser fra 2004 peker også mot 90% som et sannsynlig tall. Microsoft mener at *spyware* direkte eller indirekte forårsaker rundt halvparten av alle systemfeil (krasj) i Windows.

Spyware har mye til felles med virus, og spres via websider eller sammen med andre programmer som lastes ned. De installeres automatisk, godt ute av syne og har typisk til oppgave å samle informasjon om brukeren, programmer, aktiviteter og data på den 'infiserte' maskinen. *Adware* er en variant av *spyware* som i stedet for å samle data fungerer som leveransekanal for annonser til brukerens skjerm. I likhet med virus kan *spyware* utnytte informasjon på brukerens maskin til å spre seg videre.

Misbruk av tillit

Også verktøy fra de største aktørene i programvare-bransjen har elementer av *spyware* i seg. Dersom brukere flest – profesjonelle eller private – hadde tatt seg tid til å lese lisensavtalene fra Adobe, Microsoft, Oracle, Symantec og så videre, i stedet for blindt å akseptere dem, ville de fleste vegret seg for å ta produktene i bruk. Mens oppmerksomheten på brukersiden er rettet mot helt andre ting, forsyner leverandørene seg grovt med all slags informasjon om brukeren og hvordan systemet brukes – typisk under dekke av å skulle forbedre produkter, brukerstøtte eller annet.

Denne praksisen – eller frekkeheden, som mange vil kalle den – er en uting som fagpressen er forbausende lite opptatt av, og som bidrar til å tåkelegge grensen mellom bruk og misbruk av informasjon. Samtidig illustrerer de et viktig poeng relatert til all informasjonsinnsamling:

Tillit. Brukere flest gir gjerne fra seg informasjon dersom de har tillit til mottakeren, og anser det som sikkert at informasjonen ikke blir misbrukt.

Nettopp denne tilliten er utgangspunktet for datafisking, som vi også diskuterte i forrige utgave. Begge deler havner imidlertid på siden av vår herverende diskusjon om *spyware*, som tar utgangspunkt i at programmene installeres uten brukerens viten, og forsyner seg av informasjon som brukeren neppe ville ha gitt fra seg frivillig.

Spyware – definisjon

Spyware er programmer som i skjul installerer seg på brukerens maskin i den hensikt å samle og rapportere informasjon om bruk, programmer, lisenser, data og personen som bruker maskinen. Rapporteringen skjer tilbake til en tjener som enten bruker informasjonen direkte eller selger den videre.

Ved for eksempel å logge brukerens tastetrykk kan et slikt program på kort tid samle betydelige mengder kontonummer, passord, koder og annen informasjon som brukeren benytter i det daglige.

Markedsføring på ville veier

Spyware og *adware* er begge markedsføringsmekanismer og går i mange tilfeller hånd i hånd. En rekke selskaper har spesialisert seg på produksjon av slike programmer og utvikler samtidig lokkemidler – typisk gratisprogrammer rettet mot de interessante målgruppene – som tiltrekker seg Web-surfere. Søkjetjenester og sentraler for nedlasting av spill er gode eksempler, og i mange tilfeller er selve annonsene på slike sider mekanismen som benyttes for skjult nedlasting av programmer – typisk ved at svakheter i Internet Explorer utnyttes. Operatørene av slike tjenester får gjerne betalt fra sine oppdragsgivere per nedlasting, og store penger er involvert.

Bildet tåkelegges av det faktum at brukeren i mange tilfeller blir gjort oppmerksom på at tilleggsprogrammer blir lastet ned, og blir bedt om å akseptere dette. Beskrivelsen av programmene og deres funksjon er imidlertid så kort og mangelfull at de fremstår som harmløse eller sågar av betydelig nytteverdi. I andre tilfeller fremstilles programmene som nødvendige for å få tilgang til den funksjon eller tjeneste brukeren egentlig ønsker eller søker. Dermed beveger vi oss i et juridisk grenseland hvor det er vanskelig eller umulig å bruke lovgiving eller juss på problemene.

Bekjempelse

Vi skal ikke falle for fristelsen til å foreta et dypdykk i teknologi, metoder og tekniske risiko-momenter,¹ men i stedet konsentrere oss om det som er viktigst for de fleste av oss: Beskyttelse. Hvordan kan vi redusere eller eliminere trusselen *spyware* representerer, hva er konsekvensene og hvilke kostnader er det snakk om?

Inntil relativt nylig var 'ryddeprogrammer', som gjennomgår hva som finnes på maskinen, korrelerer Registry med filsystem, ser på automatiske oppstarts-elementer og andre typiske spor etter *spyware*, vårt eneste forsvar. Mens slike verktøy langt fra har vært verdiløse, har det lenge vært klart at veien ikke kan føre til målet. Som tilfellet er med virus, er forsvar av enkeltindivider (klienter) ikke en skalerbar løsning. De uønskede elementene må stoppes før de kommer frem til den enkelte PC, alt annet blir *too little, too late*, både med hensyn til skalerbarhet og sikkerhet.

Klient-verktøy

Verktøyene som har kommet på markedet i løpet av de siste 18-24 månedene, kan grovt inndeles i 2 kategorier eller grupper: For

Spyware, holdninger og utbredelse

Spyware er et vesentlig større problem enn de fleste er klar over. Tallene nedenfor stammer fra undersøkelser foretatt i 2. halvår 2004.

- 90% av alle Windows PCer er infiserte av *spyware*.
- I konsument-markedet er 85% av alle Windows-PCer infiserte.
- Blant eiere/brukere av infiserte systemer, er 88% ikke klar over at maskinen er 'kompromittert'.
- 75% av alle PC-eiere mener at maskinen deres er godt sikret mot infeksjon av virus, *spyware* og andre nettbaserte trusler.
- Kun 24% av PC-eierne har kunnskap om hvordan de skal forholde seg for å bli kvitt/beskytte seg mot *spyware*.
- Kun 35% av PC-brukerne kjører oppdatert antivirus-programvare.
- Halvparten av alle bredbånd-brukere har ingen brannmur. For brukere av oppringt samband har kun 7% brannmur.

1 Flere av leverandørene som utvikler og markedsfører produkter for bekjempelse av *spyware*, har laget grundige og fritt tilgjengelige WHITE PAPERS som gjennomgår de tekniske sidene av truslene. Se for eksempel www.8e6.com ("Neutralizing the Spyware Threat"), www.esafe.com ("The Spyware Epidemic: Dealing with 'legal' malicious code") og www.tippingpoint.com ("Understanding and Preventing Spyware in the Enterprise").

Selskapet **Lavasoft** har sin opprinnelse fra Tyskland tidlig på 90-tallet, og har i dag sitt hovedkvarter i Sverige. Produktene markedsføres i Norge og en rekke andre land av Norman ASA.

henholdsvis det profesjonelle marked og konsumentmarkedet. Karakteristisk for den siste gruppen er at de installeres og kjøres på brukers egen maskin, og har mange fellestrekk med brannmurprodukter. Nett-tjenesten www.download.com lister over 100 produkter i denne kategorien – en blanding av *freeware*, *shareware* og kommersielle produkter. Oversikten inneholder også en 'rating' som ved siden av antall nedlastinger gir en pekepinn om popularitet og kvalitet.

To produkter i denne gruppen som har fått spesielt positiv omtale fra eksperthold er Ad-Aware SE (www.lavasoft.com) og Spybot Search&Destroy fra Safer-networking.org.² Begge er gratis for privatbrukere og de kan gjerne brukes sammen. Kombinasjonen representerer en dramatisk sikkerhetsforbedring for systemer som tidligere ikke har hatt noen form for spyware-beskyttelse.

Samtidig er det innlysende at bruk av slike verktøy ikke er gratis rent ytelsesmessig. Programmene skal overvåke systemet kontinuerlig, og konsumerer dermed alltid ressurser. Sammen med viruskontroll, brannmur og andre løpende overvåkingstjenester blir denne 'kontrollbelastningen' signifikant. Kostnaden blir spiselig fordi den *spyware* og *adware* som fjernes, typisk konsumerte enda mer ressurser på egen hånd. Dessuten finnes slike ressurser – først og fremst regnekraft og hukommelse – typisk i overflod på dagens PCer, i alle markedssegmenter. Like fullt er det ikke til å komme forbi at vi gjerne skulle ha vært denne kostnaden foruten, hvilket er hva anti-*spyware*-produktene for det profesjonelle markedet hevder å levere.

Verktøy for proff-markedet

Produkter utviklet for proff-markedet karakteriseres ved at de angriper problemet fra nettverkssiden, med mange paralleller til nettverksbasert virus-filtrering og andre filtreringsmekanismer. Slike produkter, fra relativt ukjente spesialister som 8e6 Technologies, Tipping Point og Aladdin Knowledge Systems, føyer seg i rekken av filtre som hører hjemme i en gjennomtenkt sikkerhetsløsning, og opererer ut fra hyppig oppdaterte databaser med digitale signaturer for kjente *spyware*-programmer og deres kommunikasjons-karakteristika.

Mens enkelte produkter er komplette bokser som plugges i nettverket og stort sett klarer seg selv (*appliances*, nettapparater), er andre ren programvare som installeres på rutere eller tjenere. I tillegg til å overvåke innkommende trafikk, holder produktene et våkent øye med trafikken ut fra vårt interne nettverk – på jakt etter forbindelser som *spyware*-programmer oppretter tilbake til sin *home base*. Dersom det siste filteret er effektivt, spiller det mindre rolle hvor tett det første er – og motsatt. Sammen har de vist seg å gi gode resultater, som ikke desto mindre varierer over tid. Som tilfellet er med virus, forandrer *spyware*-programmene og mekanismene de benytter, seg løpende.

² En prøvekjøring av disse produktene på en PC som har vært eksponert for Internettet en tid, er kostnadsfritt og en lærerik øvelse som nærmest garantert byr på overraskelser dersom det er første gang spyware-deteksjon kjøres på den aktuelle maskinen.

Dette blir en langvarig krig og et kappløp mellom to sider som kontinuerlig kjemper om å være smartest.

En forsvarsstrategi

Erkjennelsen av at *spyware* er et undervurdert sikkerhetsproblem som plager nærmere 90% av alle PCer, burde være mer enn nok til å bringe utfordringen til topps på akutt-listen for de fleste sikkerhetsansvarlige. Risikomomentene og de driftsmessige utfordringene som uvegerlig følger i kjølvannet av *spyware*, er minst like alvorlige som tilsvarende for virus, og håndteringen må være deretter.

Den gode nyheten er at løsninger og produkter som bringer utfordringen under kontroll, finnes og er rimelig lett tilgjengelige. Installert og brukt riktig kan disse verktøyene klare seg med minimalt tilsyn. Det riktige stedet å begynne er å ta for seg nett-ressursene som er nevnt i denne artikkelen (se fotnote på side 5) og på den tilhørende referansesiden på vår Web-tjeneste (se side 35).

Slagplanen bør – etter at vi har akseptert at utfordringen er av akutt karakter – inneholde følgende hovedelementer, i denne rekkefølgen:

- ✓ Skaff til veie tilstrekkelig kunnskap, gjerne i samarbeid med en kompetent leverandør, til å legge en plan for hvordan utfordringen best kan håndteres for din organisasjon. Utvidelse av organisasjonens sikkerhets-policy til å dekke *spyware/adware* er en del av denne prosessen.
- ✓ Gi brukernes støttespillere på IT-siden (*help-desk*) den opplæring og bakgrunnskunnskap de trenger for å forstå problemet og for å kunne rettlede brukerne når spørsmålene kommer.
- ✓ Sørg for tilsvarende for brukerne – på et mer overfladisk nivå, men tilstrekkelig til at de for det første forstår problemet og kjenner symptomene, og for det andre oppfatter sitt eget ansvar.
- ✓ Implementér, test og sett i drift de tekniske løsningene.
- ✓ Rensk brukernes utstyr for *spyware*.
- ✓ Kontrollér effekten, foreta justeringer der det trengs.