LAVASOFT

makers of Ad-Aware

Odinsgatan 10, Göteborg

LAVASOFT

Bedrägeriprogram

och deras ekonomiska inverkan

Bedrägeriprogram - definition

Ett medel med vilket en bedragare kan utföra en bedräglig handling i syfte att genera personlig monetär vinning. Bedrägeriet sker på bekostnad av en annan vilseledd eller lurad individ.

Begreppet Bedrägeriprogram innefattar i detta avseende falska Antivirus- och Antispyware-applikationer som är konstruerade med avsikt att lura användare.

Vi har dock valt att använda begreppet **Rogue-applikationer** istället då det är mer internationellt gångbart.

LAVASOFT

Paradigmskifte

- Slutet av 2005 skedde en omfattande förändring
  Rogue-applikationerna äntrade den globala scenen
- SpyAxe, SpyFalcon, SpywareStrike och Winfixer var först ut
- Klon-fenomenenet tog sin början
- CWS, Cool Web Search, som distribueringsmedel

Nedladdare och dirigenter

- Zlob-trojanen med nedladdnings- och dirigent funktion
  Emanerade i slutet av 2005
- Koppling mellan Zlob-trojanen, fake-codecs och porr-sidor
- Win32.TrojanDownloader.Zlob och Win32.Trojan.DNSchanger
- Små frekventa förändringar i programkoden för att undvika detektion
- 2007 – 2008 möjlig konkurrens mellan olika fake-codecs

Infektionskedjan länk för länk

IE Antivirus - TotalSecure 2009

Infektionskedjan länk för länk

IE Antivirus - TotalSecure 2009

Infektionskedjan länk för länk

IE Antivirus - TotalSecure 2009

Infektionskedjan länk för länk

IE Antivirus - TotalSecure 2009

Infektionskedjan länk för länk

IE Antivirus - TotalSecure 2009

Vad händer sedan?

- Användaren presenteras med frekventa ”System Alerts”
  Hårdkodade, påhittade, infektioner listas för användaren

- Användaren uppmanas att registrera/köpa produkten
  Endast den registrerade versionen sägs kunna rensa ”infektionerna”
  Det eventuella köpet administreras oftast via specifika https-sidor

Andra typer av Rogue-applikationer

- BraveSentry
  - Win32.Worm.Zhelatin – Win32.TrojanDownloader.Tibs
  - Peer to peer Botnet, decentraliserad struktur, svåra att stänga ner
  - Lång levnadstid

- XP Antivirus 2008
  - Sprids via exploits, sårbarheter i Windows eller Internet Explorer
  - Efterliknar Windows-funktioner för att lura användaren

- Adware Alert och SpywareBot
  - Utnyttjar legitima AntiSpyware applikationers namn

Det finns också andra Rogue-applikationer som efterliknar gränssnitten hos legitima antispyware- och antivirus program

LAVASOFT

Botnät som spridningssystem

Botnät – Botnet

- Går att hyra för olika uppgifter, t.ex. Spam och Rogue-applikationer
- Stort antal noder, t.ex. Storm-botnätet 250 000 – 50 miljoner noder
- De smittade noderna kallas ”Zombie-datorer”
- Möjlighet till stora ekonomiska vinster med relativt små kostnader

Ökningsfrekvens

Antalet upptäckta Rogue-applikationer

- 2005 detekterade vi 11 Rogue-applikationer
- 2006 detekterade vi 28 nya
- 2007 detekterade vi 102 nya
- 2008, fram till sept., har vi detekterat 182 nya

Ökningen motsvarar 1645 %

Spridningsmönster

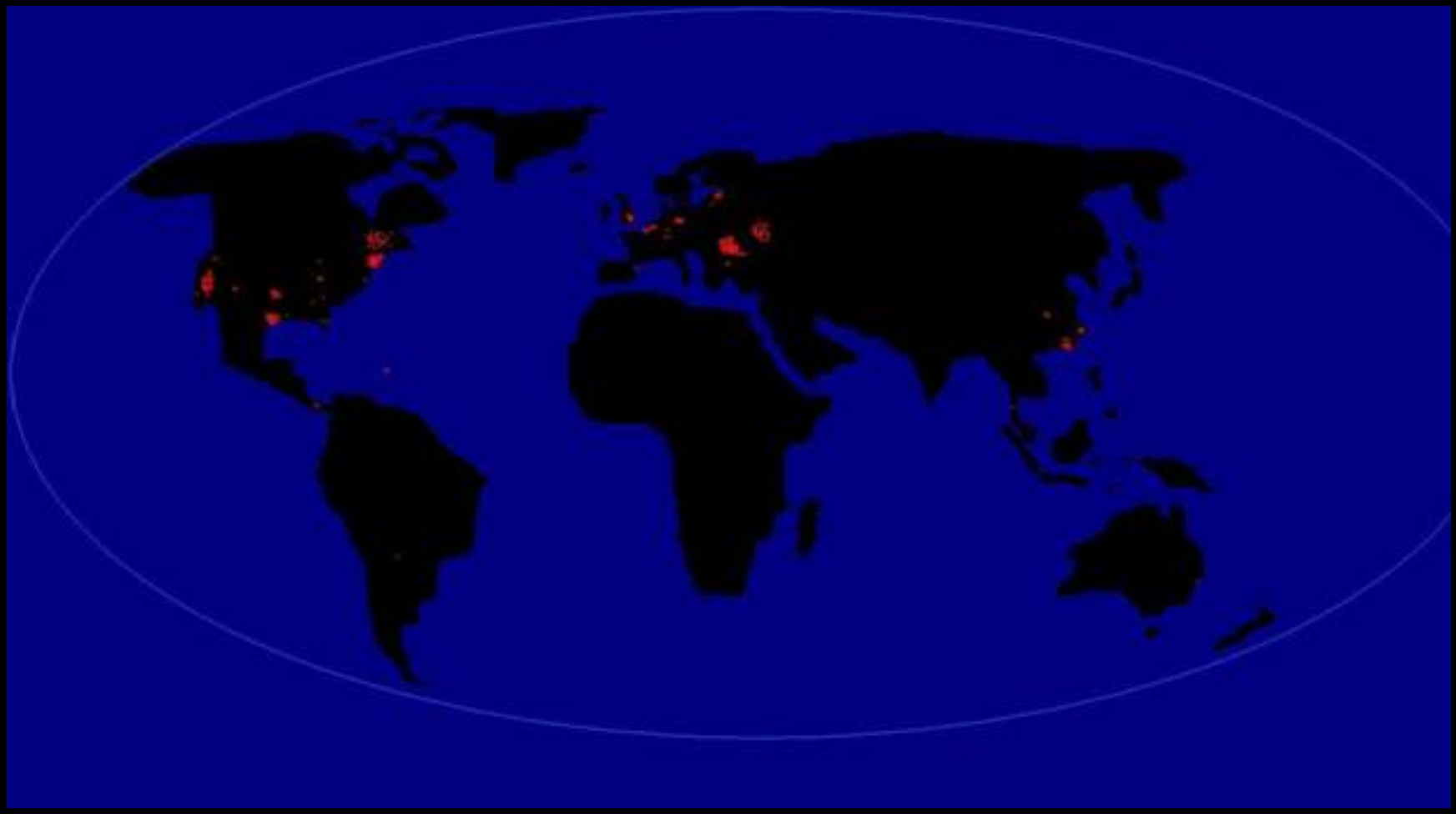
- Vi har sett en tydlig ökning av spridningen av Rogue- applikationer från USA

- Över 30% av moderdomänerna till Rogue-applikationer mellan den senare delen av 2007 och fram till idag har sitt säte vid den nordamerikanska västkusten

- Ökningen kan ha sin grund i att tidigare Rysk verksamhet med möjliga kopplingar till upplösta RBN:s (Russian Business Network) tagit ny fart i västra USA.

Följande karta visar spridningshärdarna från 2005 – 2008 ...

Spridningsmönster



Ekonomisk inverkan

Individnivå

- Ca. 300-400 kr för att licensiera en Rogue-applikation
- Ev. Stulna kreditkorts- och/eller bankuppgifter
- Kan resultera i en privatekonomisk katastrof

Övergripande nivå

- Domännamnsregistratorer, ISP och de kriminella aktörerna kan profitera på den här typen av verksamhet.
- Den totala ekonomiska inverkan kräver att alla parters omsättning räknas in i den totala. Svårt att få full insyn i ”mörkerekonomin”.

Individen = den stora förloraren

Möjliga motåtgärder

Individnivå

- Ökad insikt/kunskap om nätbedragarnas strategier
- Förbättrad pedagogisk information via pålitliga säkerhetsföretag, media etc.
- Uppdatering av systemet med tillgängliga säkerhetspatchar
- Andvändning av brandvägg för ökad kontroll av in- och utg. trafik
- Kontroller av det egna systemet via användandet av t.ex. MBSA, Microsoft Baseline Security Analyzer, eller via tester av systemsäkerheten på webblatser såsom ”ShieldsUp!”, grc.com
- Använda adekvata anivirus/antispyware program

Möjliga motåtgärder

Övergripande nivå

- Översyn av ICANN:s (Internet Corporation for Assigned Names and Numbers) godkännande av domännamnsregistratorer

- Ökat samarbete mellan domännamnsregistratorer och ISP

Ökad kontroll av nätverkstrafik och domäninnehåll, via ovan nämda aktörer, får inte missbrukas så att det inskränker på individers rätt till personlig integritet

LAVASOFT

Fortsättning följer?