



Denne forelesningsøkten vil bli tatt opp og lagt ut i emnet i etterkant.

Hvis du ikke vil være med på opptaket:

	La være å delta med webkameraet ditt.
	La være å delta med mikrofonen din.
To: Marianne Sundby (Privately) Type message here...	Still spørsmål i Chat i stedet for som lyd. Hvis du ønsker kan spørsmålet også sendes privat til foreleser.



Høyskolen
Kristiania

TK2100: Informasjonsikkerhet

Pensum (2011):
Kapittel 4 (s. 167-214)

Pensum (2014):
Kapittel 4 (s 173 -214)

Nätt & Heide: Kapittel 7

Fjerde forelesning:

MALWARE

Hva er **malware**?

- **Malicious Software**

- Fellesbetegnelse på “Ondsinnede programvare” som utfører uautoriserte og (oftest) skadelige handlinger



Klassifikasjon («historisk»)

- Vi kan dele **malware** opp i ulike **typer** ut fra hvordan den spres og hvordan den skjuler seg.
- **Spredning**
 - **Virus**: Virus endrer eksisterende filer eller systemer, koden kan ikke leve eller spre seg alene
 - **Orm**: automatisk spredning fra maskin til maskin over nettet
- **Skjuler seg**
 - **Rootkit**: endrer OS for skjule nærvær
 - **Trojaner**: Nytteprogram som skjuler ondsinnede operasjoner (f.eks. keylogger)
- **«Nyttelast» (payload)**
 - Alt fra humor/irritasjon til ran av maskinkraft og identitetstyveri

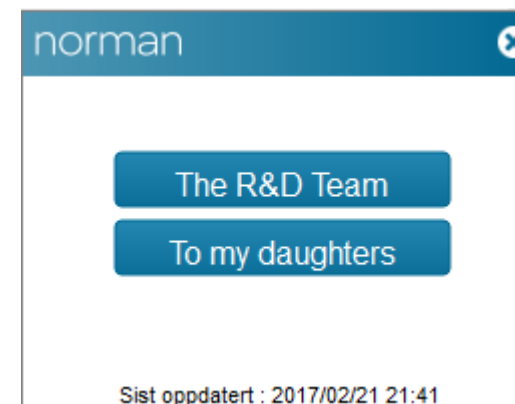
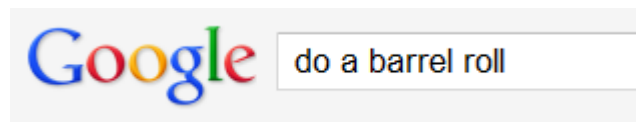
Innside-angrep

«Den glemte trusselen»

- Innside-angrep
 - skyldes/tilrettelegges av noen som er del av organisasjonen som kontrollerer eller bygger tjenesten som skulle vært beskyttet
 - «Utro tjenere»
- Kan være malware som utnytter sikkerhetshull som er lagt inn med vilje av en programmerer
- Mest aktuelt for bedrifter og deres kunder.

Bakdører («backdoor/trapdoor»)

- En skjult metode/kommando i et program som (typisk) tillater en bruker å utføre handlinger han/hun normalt ikke har tillatelse til
- Programmet oppfører seg vanligvis helt som forventet
- Når aktivert så gjør programmet noe du ikke forventet, f.eks. hever privilegier
- Vennlig utgave:
«Easter Eggs»



Logikkbomber

- **Logikkbomber** utfører en handling først når en bestemt **betingelse** inntreffer
- Eksempel («klassisk»)
 - En programmerer legger inn en betingelse om programmet skal krasje og alt slettes dersom han ikke er med i to lønnsutbetalinger på rad...



Symantec's Vontu avdeling hevder

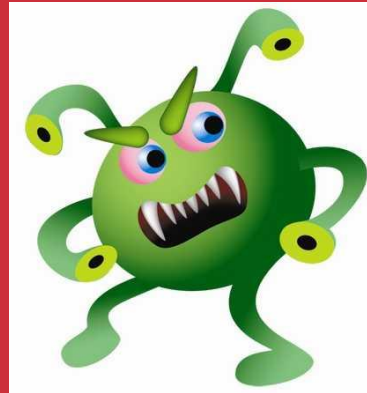
- 1 av 500 eposter inneholder konfidensielle data.
- 66% hevder at kolleger, ikke hackere, er største trussel mot forbrukeres privatliv
- 46% sier at det er enkelt å fjerne sensitive data fra bedriftens database
- 32% vet ikke hva bedriftens sikkerhets-policy er...

Forsvar mot **insider**-angrep

- Unngå «single points of failure»
- Bruke (manuell) kode-gjennomgang
- Bruk arkiveringsverktøy og rapport-verktøy
- Begrens tillatelser og autorisasjoner
- Fysisk sikring av kritiske systemer
- Overvåk ansattes adferd
- Stålkontroll på alt som installeres

- Eller: Open Source (ref: Silent Circle)

Virus

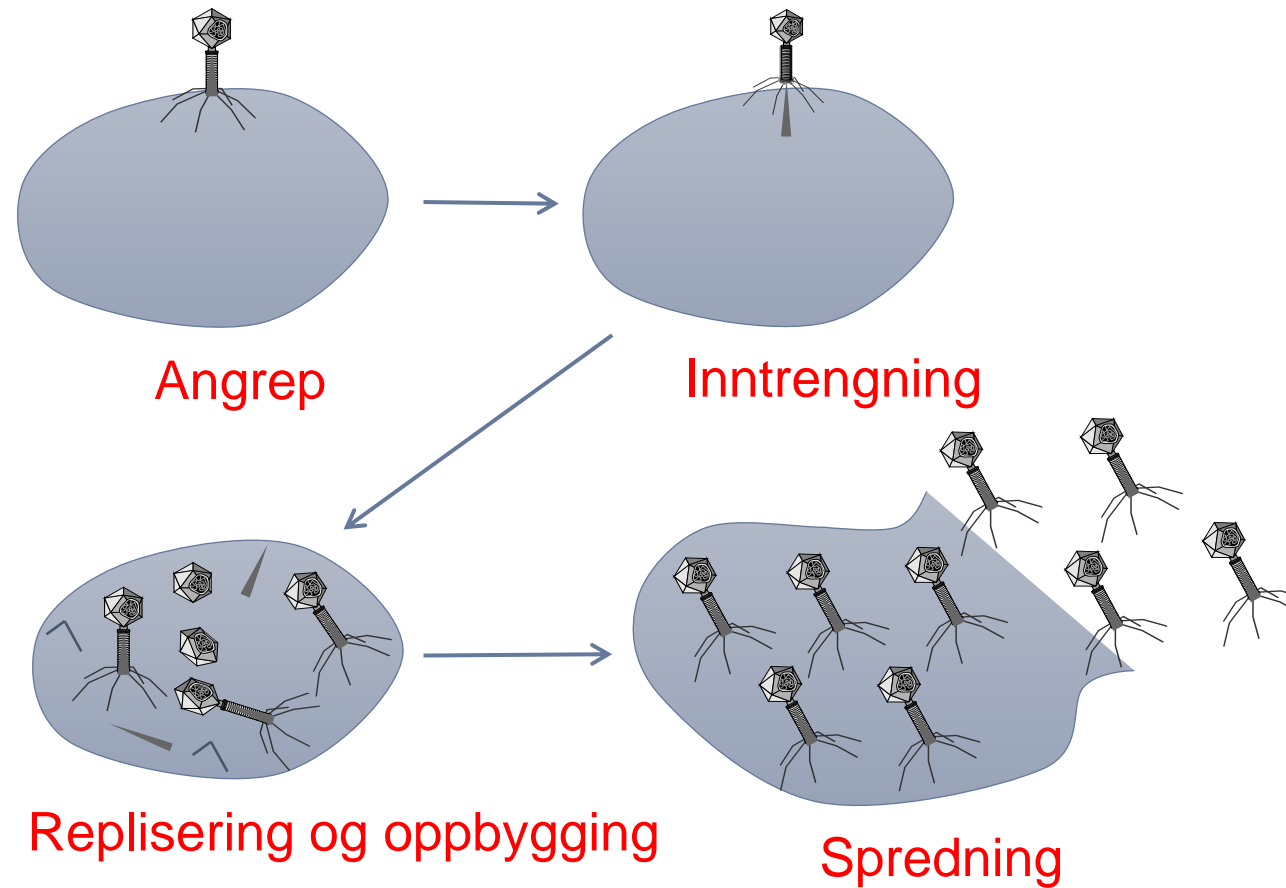


Hva er et computer virus?

- Et program som kan **replisere** seg selv
 - ved å endre andre filer/program
 - ved å **infisere** dem med kode
 - som kan **formere** seg videre
- Det er evnene til å **formere seg LOKALT** som skiller virus fra andre typer malware
- Krever vanligvis innledende **brukermedvirkning** for å formere seg
 - Klikke på en link og godta installasjon
 - Åpne epost-vedlegg
 - Dele en **minnepinne**, eller annet USB-utsyr

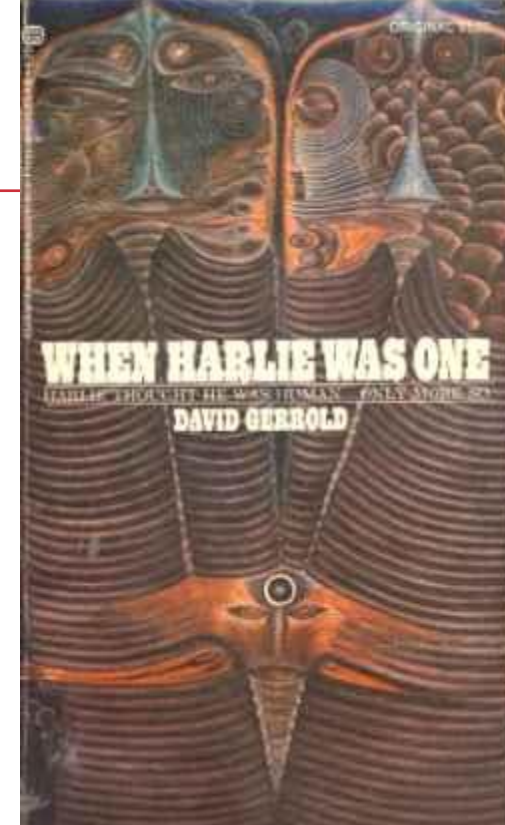
Analogi fra biologien

- Ligner litt på biologiske virus



Forhistorie

- I David Gerrolds AI-roman «*When HARLIE was One*» (1971) forekommer programmet VIRUS, som reproducerer seg selv
- Adleman (A'en i RSA-krypteringsalgoritmen) foreslo begrepet (1984) for Fred Cohen, som skrev sin PhD på teorien bak
- De første PC-virus som ble observert på 1980-tallet var typisk «boot-virus» som infiserte boot-sektoren på disketter og (etter hvert) harddisker.



Tradisjonelle datavirus

- I dag er det mer vanlig med ormer og trojanere; malicious filer som er i stand til å leve et selvstendig liv uten en host-prosess
- Ormer har eksistert lengre enn PCer, og første registrerte malware kom i 1971 og kalles "The Creeper Program" og spredde seg over ArpaNet
- Brain krediteres som verdens første "PC virus" (1986), og senere samme år klarte man for første gang å infisere exe filer med Suriv-02
 - Exe filer var først ansett som et trygt format fordi det var så kompleks at ingen ville kunne klare å infisere dem, i motsetning til com filer som er ren maskinkode...
 - Noen krediterer Old Yankee som den første exe fil infektoren
- Flere farlige virus kom ut på denne tiden:
 - AIDS Trojan (1989); krypterte hele disken din
 - Dark Avenger (1989); overskrev random deler av disken 1/16 ganger viruset kjørte
 - Jerusalem (1987); Sletter filer på maskinen på Fredag 13nde...
 - Tequila (1991); Polymorph virus som var stealthet, og veldig vanskelig å oppdage

Brain

- ©Brain –
Januar 1986
- Skrevet av to
brødre i Pakistan
for å beskytte ©
på program-
varen for hjerte-monitorering de solgte
- Inneholdt telefonnummeret deres

```

PC Tools Deluxe 14.22      Disk View/Edit Service
Path=A:                    Absolute sector 0000000, System BOOT

Displacement  Hex codes  ASCII value
0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20  .8J04: * 0
0016(0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F  Welcome to
0032(0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20  the
0048(0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050)  20 20 63 29 20 31 33 38 36 20 42 61 73 69 74 20  (c) 1986 Basit
0096(0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74  & Amjad (pvt) Lt
0112(0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20  d.
0128(0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20  BRAIN COMPUTER
0144(0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49  SERVICES..730 NI
0160(00A0)  54 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41  2AM BLOCK ALLAMA
0176(00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20  IQBAL TOWN
0192(00C0)  20 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52  LAHORE
0208(00D0)  45 20 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E  E-PAKISTAN..PHON
0224(00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38  E :430791,443248
0240(00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,280530.

Home=begin of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
  
```

Welcome to the Dungeon © 1986 Basit * Amjad (pvt) Ltd. BRAIN

- COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-
PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS....
Contact us for vaccination...

Mengden av virus

- Alan Solomon, 1993:

There will be more viruses - that's an easy prediction. How many more is a difficult call, but over the last five years, the number of viruses has been doubling every year or so. This surely must slow down. If we say 1500 viruses in mid-1992, and 3000 in mid-1993, then we could imagine 5000 in mid 1994 and we could expect to reach the 8,000 mark some time in 1995.

The glut problem will continue, and could get sharply worse. (...) The biggest nightmare for all anti-virus people is glut. There are only about 10-15 first class anti-virus people in the world, and most of the anti-virus companies have just one of these people (some have none). It would be difficult to create more, as the learning curve is very steep. The first time you disassemble something like Jerusalem virus, it takes a week.

Scanners will get larger - more code will be needed because more viruses will need hard coding to scan for them. The databases that scanners use will get larger; each new virus needs to be detected, identified and repaired. Loading the databases will take longer, and some programs will have memory shortage problems.

(...) But if you are running Windows, you have run software on the hard disk. (...) If there is a virus in memory, you cannot trust what the computer is saying (...). Windows will make antivirus software less secure.

The R&D effort to keep scanners up-to-date will get more and more. Some companies won't be able to do it, and will decide that scanning is outdated technology, and try to rely on checksumming.

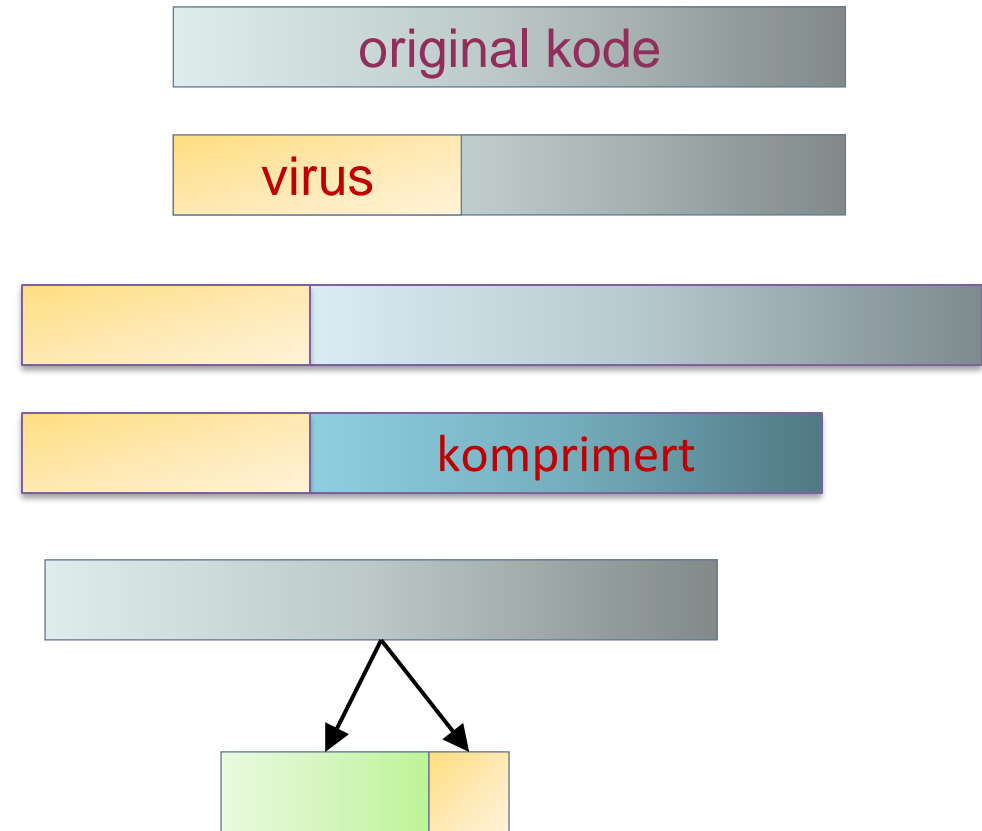
- Dommedagsprofetier? Tja, i følge test instituttet AV-TEST kom det bare i 2019 145 millioner nye datavirus (malware), totalt i dag er det ansett at det finnes 1018 millioner forskjellige malware!

Virus: Livsfaser

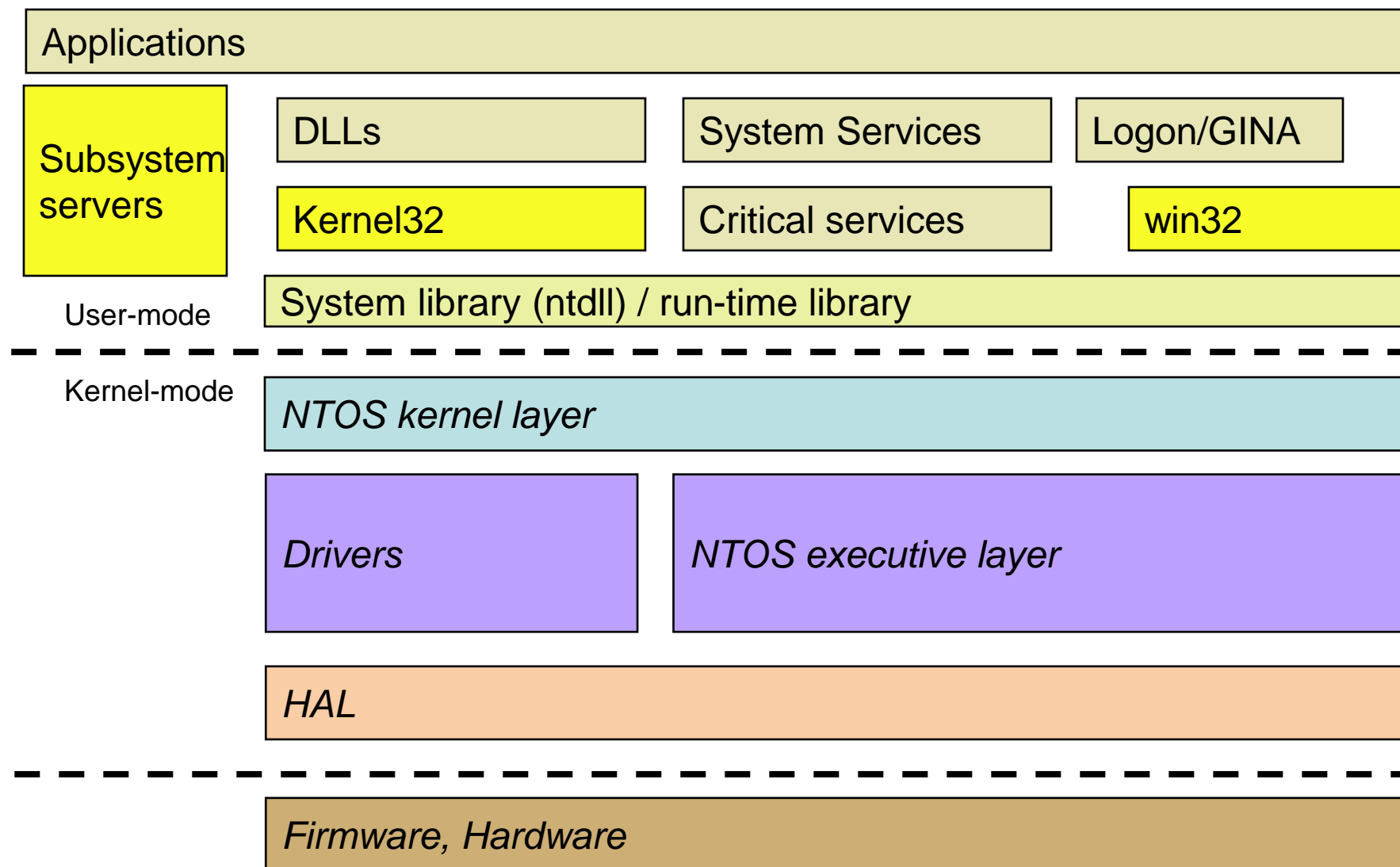
- **Dvale-fasen**
 - Offeret er infisert, men viruset ligger lavt og unngår å bli oppdaget
- **Sprednings-fasen**
 - Viruset repliserer seg selv, og infiserer flere filer (og nye systemer)
- **Avtrekker-fasen**
 - En logisk betingelse («avtrekker») får viruset til å begynne å utføre sin intenderte handling
- **Aksjons-fasen**
 - Viruset utfører handlingen det var designet for: «nyttelasten» («payload»)
 - Alt fra å vise frem et tåpelig bilde til å slette/kryptere hele filsystemet

Infeksjonstyper

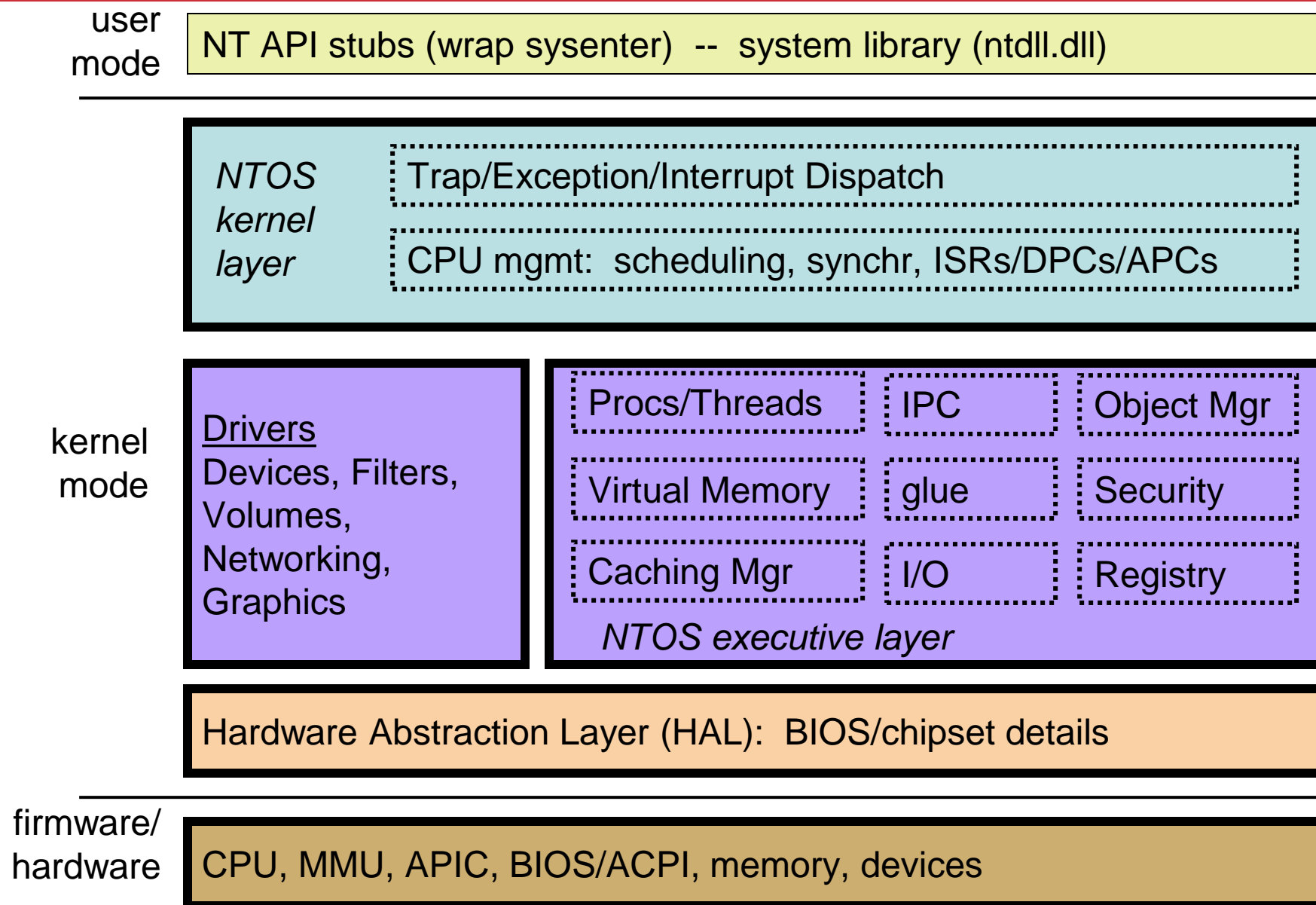
- **Overskriving**
 - Ødelegger opprinnelig kode
- **Pre-pending**
 - Beholder opprinnelig kode
 - Kan komprimere den
- **Biblioteksinfeksjon**
 - Tillater virus å være minne-resistente
 - F.ex. kernel32.dll
- **Makro-virus**
 - MS Office dokumenter
 - Erstatter gjerne hoved dokument-malen



Windows arkitektur



Win: Kjernemodus arkitektur



Dynamic Link Library

- DLLer har en export-tabell med liste over metoder (systemkall) og adressene de ligger på
- Mange virus enten endrer tabellen slik at den kaller viruset kode i stedet, eller legger inn ondsinnet kode i selve DLen
- Typiske offer: kernel32.dll, ntdll.dll, kernelbase.dll (64bit)

```
C:\Program Files (x86)\Microsoft Visual Studio 10.0\VC>dumpbin "C:\WINDOWS\system32\kernel32.dll" /exports /more
Microsoft (R) COFF/PE Dumper Version 10.00.40219.01
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file C:\WINDOWS\system32\kernel32.dll
File Type: DLL

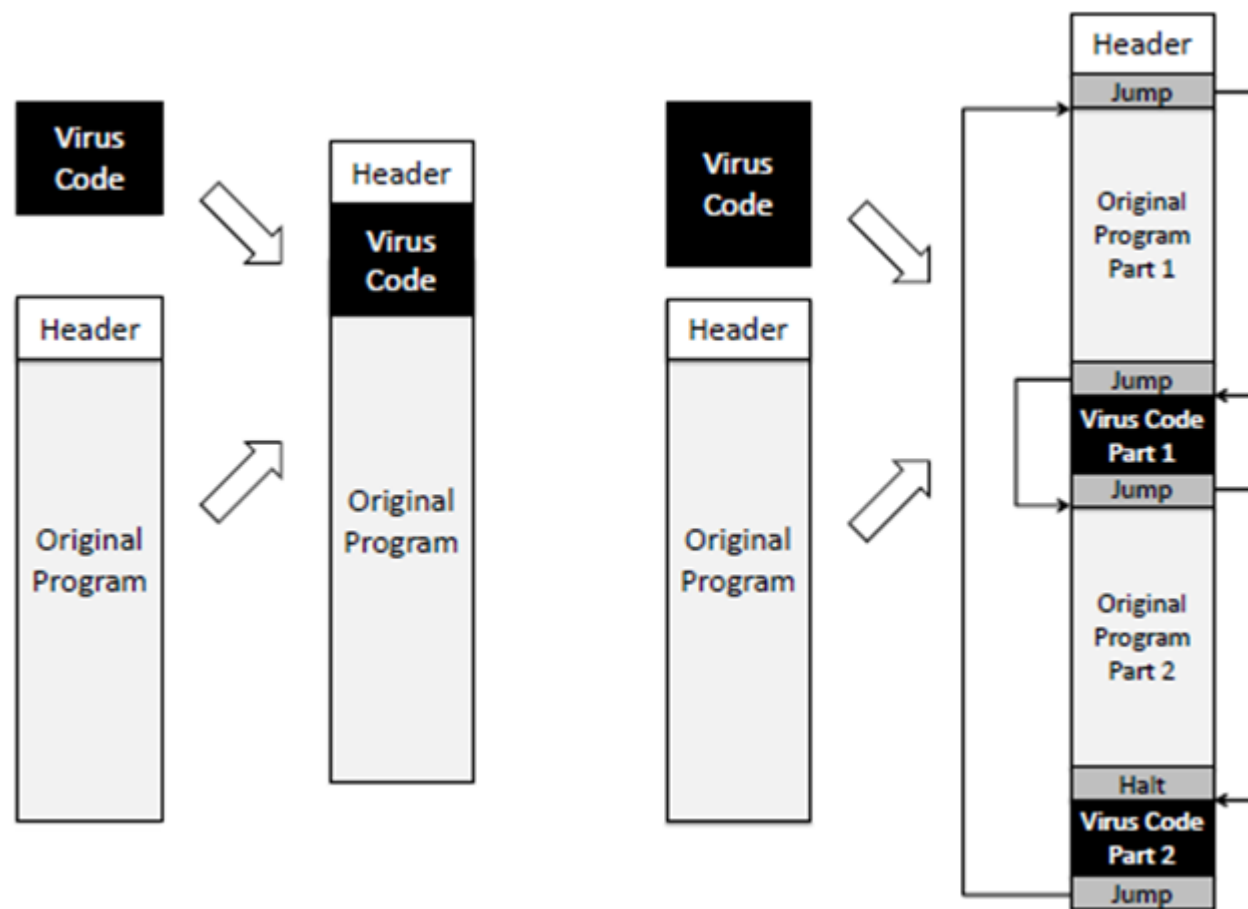
Section contains the following exports for KERNEL32.dll
 00000000 characteristics
 4E20FCBC time date stamp Sat Jul 16 04:51:40 2011
 0.00 version
 1 ordinal base
 1390 number of functions
 1390 number of names

ordinal hint RVA      name
1 0 AcquireSRWLockExclusive (forwarded to NTDLL.RtlAcquireSRWLockExclusive)
2 1 AcquireSRWLockShared (forwarded to NTDLL.RtlAcquireSRWLockShared)
3 2 000042F0 ActivateActCtx
4 3 00066910 AddAtomA
5 4 000668B0 AddAtomW
6 5 0006AB80 AddConsoleAliasA
7 6 0006ABF0 AddConsoleAliasW
8 7 AddDllDirectory (forwarded to api-ms-win-core-libraryloader-l1-1-0.AddDllDirectory)
9 8 0004B290 AddIntegrityLabelToBoundaryDescriptor
10 9 000957B0 AddLocalAlternateComputerNameA
11 A 0008FC80 AddLocalAlternateComputerNameW
12 B 000486F0 AddRefActCtx
13 C 0004B2C0 AddSIDToBoundaryDescriptor
```

Visual Studio
verktøyet
dumpbin
kan vise hvilke
kall som ligger i
DLen

Grad av kompleksitet

- Virus kan gjemme seg inne i annen kode på ulike måter



Hvordan oppdage virus?

- Den mest fundamentale teknikken er å finne **signaturer** for kjente virus og søke etter disse
- Forutsetter at man finner **karakteristiske kodesnutter** i viruset som man så kan sette opp antivirus-programmet til å søke etter.
- Programmer som matcher signaturen legges i **karantene**
- Fungerer bare med oppdatert oversikt over signaturer



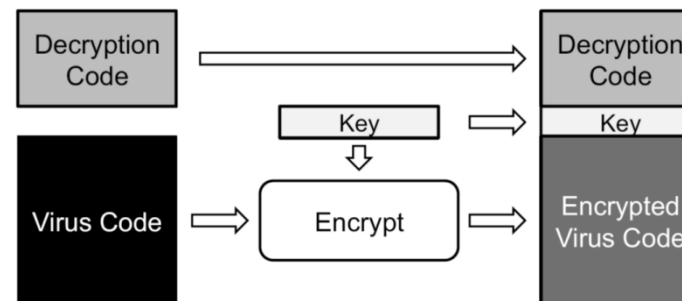
Virus and spyware definitions: **Up to date**

Hvordan oppdage virus #2

- Problemet i dag er at det kommer så mange virus hver dag (**375.000** nye virus HVER DAG...)
- Alle antivirus selskap **deler** databaser over kjente virus, alle som bidrar med feed av virus får være med i **samarbeidet** (CARO)
- I tillegg kan man kjøpe **feeds** av forsknings institutter (Virus Total, AV Test, VB)
- Alle filer fra kjente feeder blir lagt inn i virusdatabasen som en **checksum**

Teknikker for å gjemme seg

- **Krypterte** virus
 - **Dekrypteringsmotor** + kryptert virus
 - Tilfeldig generert krypteringsnøkkel
 - Antivirus søker etter dekrypteringsmotoren
 - Ofte bare for å skjule koden, men kan gi:
- **Polymorfe** virus
 - Virus legger inn tilfeldige variasjoner i koden sin før den sprer seg videre
 - En polymorphic engine trengs for å dekode viruset før det kan kjøre
 - Kan detekteres med CPU-emulator
 - Må finne signatur basert på evnen til å endre seg selv
- **Metamorfe** virus
 - Forsøker å gjemme seg og være vanskelige å finne en signatur på ved «obskurifisering»:
 - endre rekkefølgen på instruksjoner
 - Legge inn unyttige instruksjoner
 - Omstrukturere indre metode-kall
 - Kan bruke statistiske metoder for å finne sannsynlige virus ut fra et bestemt antall under-signaturer



- Å gjemme seg for anti-virus handler da ofte om å **skjule signaturen**, eller gjøre den vanskelig å generere

Virus eksempler

- Jerusalem (DOS, 80-tallet)
 - Slettet alle programfiler som ble kjørt på fredag den 13.
- Melissa
 - Første som spredde seg via epost
 - Makro-virus i Word og Excel
 - Spredde seg ved å maile infiserte dokumenter til de 40-50 øverste i adresseboken på maskinen
- W32.Sality
 - Forholdsvis moderne
 - Deaktiverer antivirus og infiserer eksekverbare filer
 - Kopler seg til malware-sites og laster ned annen malware
 - http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99

Ormer

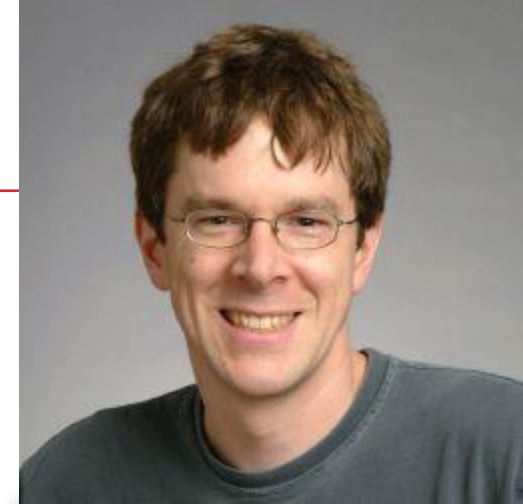


Hva er en orm («Worm»)?

- Malware som **sprer kopier** av seg selv **uten å infisere** andre program, og vanligvis uten menneskelig medvirkning
- Ikke virus siden de ikke infiserer eller endrer LOKALT (filer eller bootsektorer)
 - men begge deler spres ved selv-replisering
- I de fleste tilfeller vil ormen ha en ondsinnet **nyttelast (payload)**
 - Installere bakdør
 - Slette filer

Historikk

- Den «første» internett-ormen ble skrevet av en student (Robert Tappan Morris), og slapp løs 2. November 1988
 - Utnyttet svakheter i Unix sendmail, dfinger og rsh/rexec, samt svake passord
 - Hevdet selv at han bare ville sjekke ut hvor mange maskiner som var tilknyttet Internett
 - Ble til et DoS-angrep fordi den reinfiserte maskiner 1 av 7 ganger og spredde seg så raskt at den tok ned ca 10% av alle Unix-servere
 - Morris fikk 3 års betinget fengsel og underviser nå ved MIT



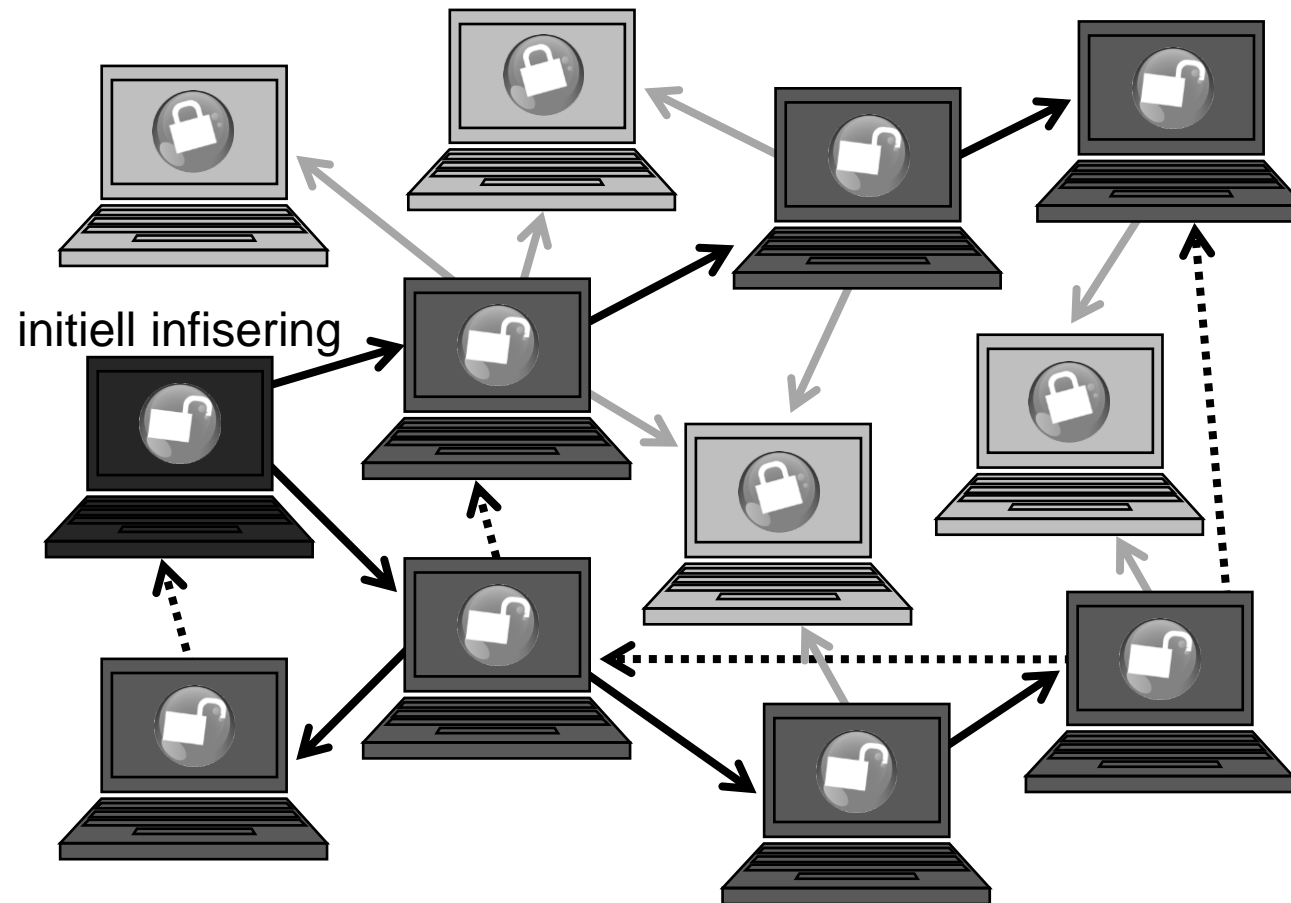
- 4. mars 2000 kom 'ILOVEYOU' ormen – og endret "alt"
 - Den første malware som spredde seg gjennom epost
 - Brukeren måtte manuelt åpne en fil i eposten
 - Egentlig ikke en skadelig malware, den bare spredde seg...
 - 50 millioner PCer ble infisert i løpet av 9 dager!
- 13. Juli 2001 infiserte 'Code Red' Microsoft IIS servere
 - Helt ny orm som spredde seg automatisk mellom servere på Internet, og som kun levde inne i Internet Information Server
 - Utførte Denial of Service attacks mot flere amerikanske nettsteder
- 'Nimda' ormen fulgte opp og satt standarden for moderne malware
 - Spredning gjennom; epost, nettverks shares, IIS spredning (som Code Red), browsing på infiserte servere, gjennom bakdører fra andre ormer

Orme-utvikling

- Finn en svakhet i OS/programvare som ikke har blitt patchet (Zero-day attack)
- Skriv kode som
 - Utnytter svakheten (typisk stack/buffer overflow)
 - Generer en liste over mål
 - Tilfeldige maskiner på nettet
 - Maskiner på LANet
 - Installerer og eksekverer nyttelasten
 - Legg ormen inn som en tjeneste/daemon i OS
 - Sjekker/rapporterer om en host-maskin er infisert
- Utplasseres typisk fra et botnet
- Virkemåten er da:
 - Generer liste over blinker/mål
 - For hver host på listen
 - Sjekk om infisert
 - Sjekk om sårbar
 - Infiser
 - Gjenta

Spredning av ormen

- Ormen sprer seg ved å finne og identifisere sårbare host-maskiner
 - Den må finne ut om maskinen er sårbar (Scanne for OS)
 - Den må kunne sjekke om maskinen allerede er infisert (få rapport)

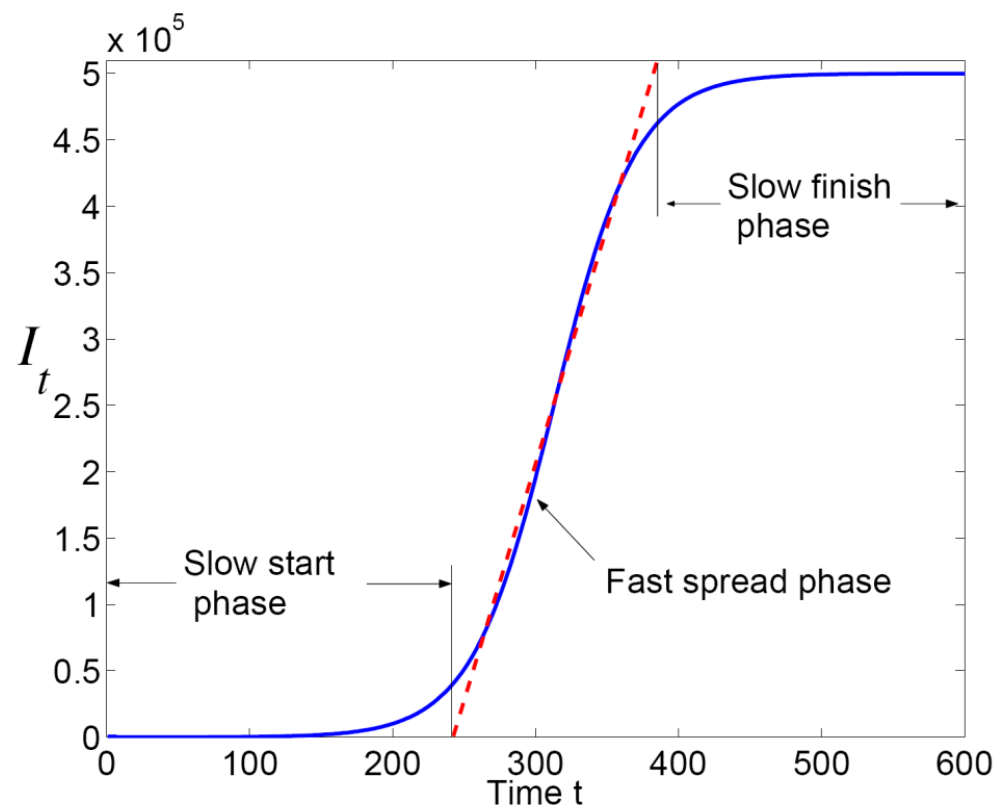


Spredning: Teori

- Sprer seg akkurat som pest eller influensa, så vi kan bruke en vanlig epidemiologisk modell
 - N : totalt antall sårbare hosts
 - $I(t)$: antall infiserte hosts ved tidspunkt t
 - $S(t)$: antall sårbare hosts ved tidspunktet t
 - $I(t) + S(t) = N$
 - β : infeksjonsrate
- Differensialligning for $I(t)$:
$$dI/dt = \beta I(t) S(t)$$
- Mer nøyaktige modeller justerer også infeksjonsraten over tid

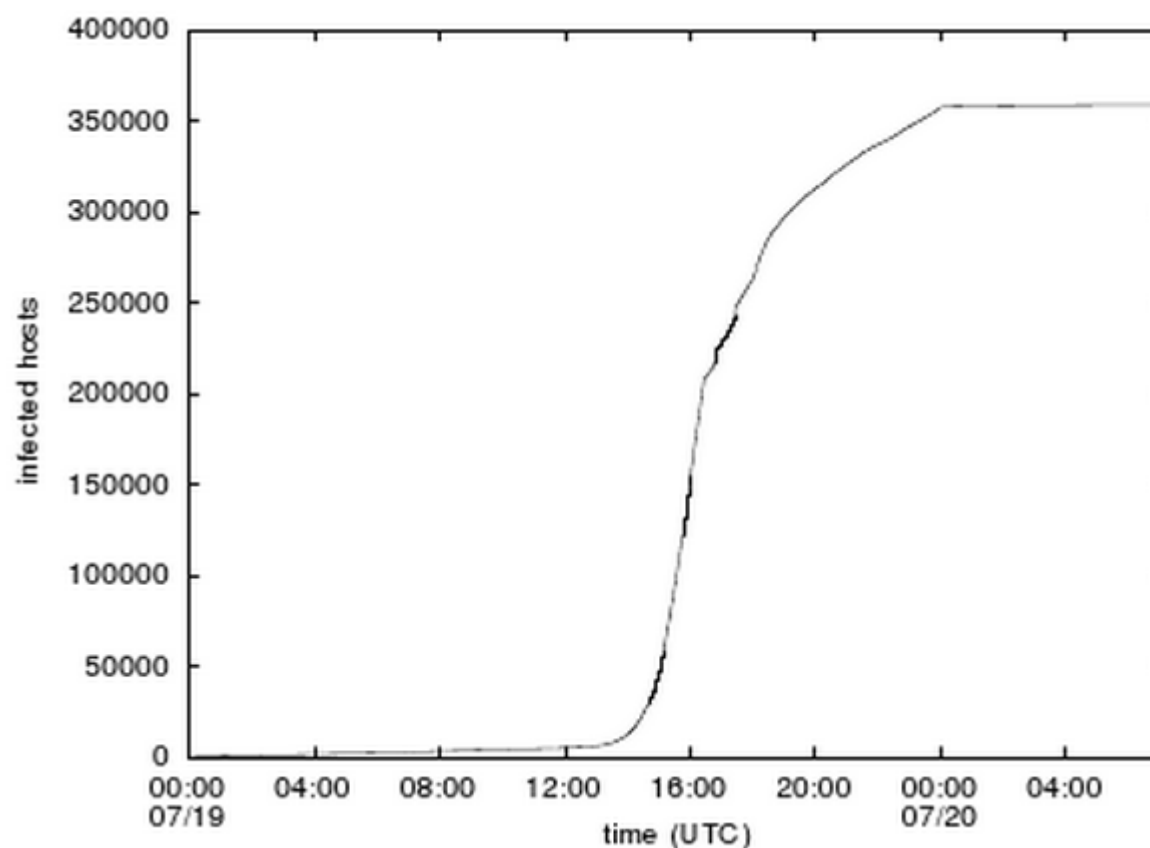
Kilde:

Cliff C. Zou, Weibo Gong, Don Towsley, and Lixin Gao. [The Monitoring and Early Detection of Internet Worms](#), IEEE/ACM Transactions on Networking, 2005.



Spredning i praksis

- Antall unike IP-adresser infisert ved første utbrudd av *Code Red I* v. 2, 19.-20. Juli 2001



Kilde:
David Moore, Colleen Shannon, and Jeffery Brown. [Code-Red: a case study on the spread and victims of an Internet worm](#), CAIDA, 2002

- Nyttelasten endret hovedsiden:

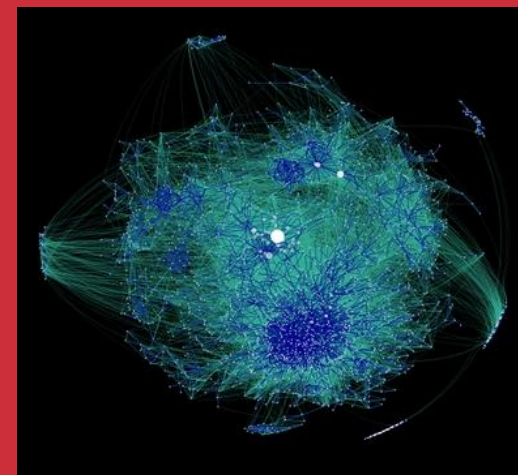
- Prøvde seg ukritisk på alt med åpen port 80
- Endret adferd ut fra dato:
 - 1.-19. Prøve å spre seg
 - 20.-27.: Kjøre DoS-angrep mot utvalgte IP-adresser (f.ex. Det Hvite Hus)
 - 28.- : Hvile
- Microsoft hadde sluppet patchen en måned **før** første angrep!!

Win32.Worm.Conficker

- Oppdaget i November 2008
- Rammet Vista, XP SP2 og Windows 2003 SP1
 - Utnyttet RPC («Remote Procedure Call») og fikk kjørt kode
 - Scannet forsiktig etter mulige offer
 - Benyttet UPnP til å passere routere
 - Oppdaterer seg selv og kjører eget P2P-nettverk
 - Slår av antivirus, filtrerer bort webtrafikk til sikkerhetsfirma og slår av Windows egne sikkerhetsmekanismer
- Fremdeles å finne på maskiner som ikke har vært patchet (typisk «tyvkopiert Windows»)



ssdpapi.dll	WINDOWS\system32	34816
ssdpsrv.dll	WINDOWS\system32	71680
ssflwbox.scr	WINDOWS\system32	393216
ssmarque.scr	WINDOWS\system32	20992
ssmypics.scr	WINDOWS\system32	47104
ssmyst.scr	WINDOWS\system32	18944
sspipes.scr	WINDOWS\system32	610304
sssplt30.ocx	WINDOWS\system32	177608
ssstars.scr	WINDOWS\system32	14336
sstext3d.scr	WINDOWS\system32	679936
Status.MPF	WINDOWS\system32	63296
stclient.dll	WINDOWS\system32	59392
stdole32.tlb	WINDOWS\system32	7168
sti.dll	WINDOWS\system32	68096
sti_ci.dll	WINDOWS\system32	136704
stimon.exe	WINDOWS\system32	14848
stobject.dll	WINDOWS\system32	121856
storage.dll	WINDOWS\system32	4208
storprop.dll	WINDOWS\system32	74752
streamci.dll	WINDOWS\system32	8192
strmdll.dll	WINDOWS\system32	8192

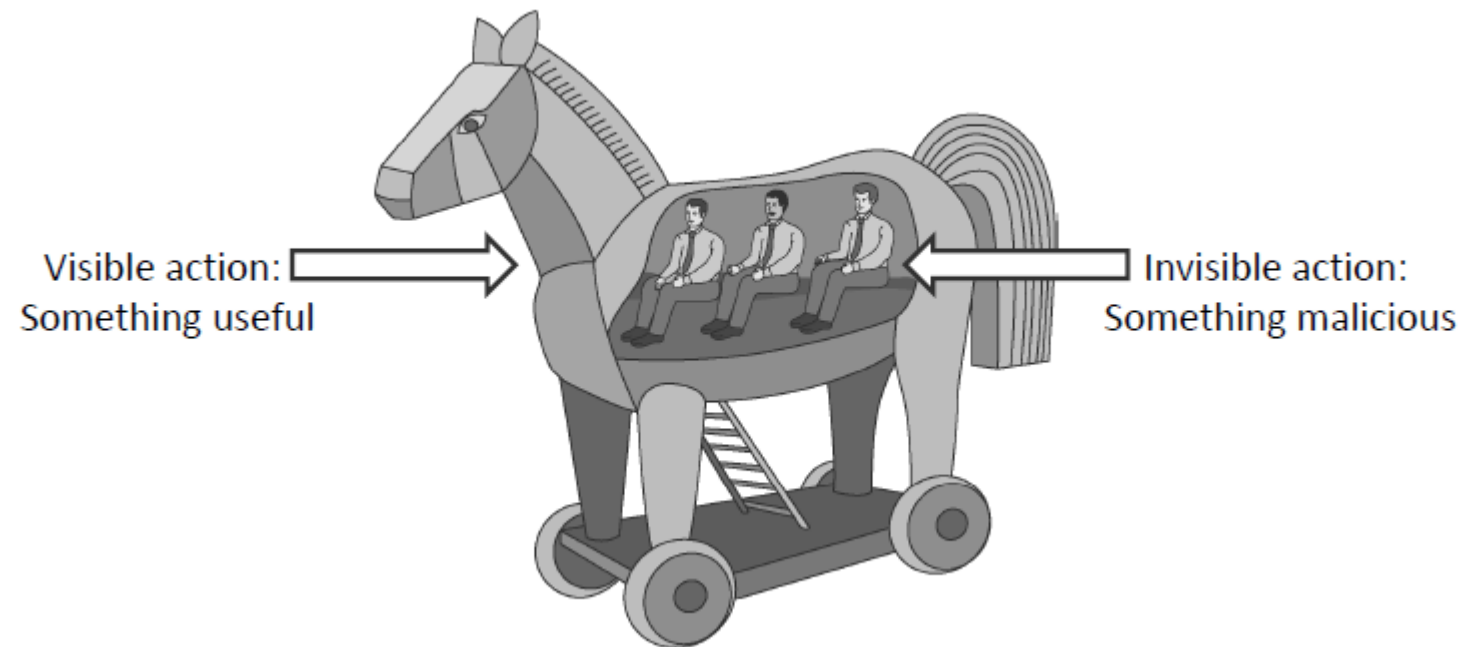


Trojanere
Rootkits
Botnets (zombies)
Ad- og Spy-ware



Trojanske hester

- Malware som **ser ut** til å utføre en **nyttig** jobb, men som **i tillegg** gjør noe ondsinnet
 - F.ex. starter en keylogger («tastaturavlytter»)
- Trojanere installeres ofte som en del av nyttelasten til annen malware
 - men kan også installeres av bruker/administrator med overlegg eller ved uhell



Eksempler: Trojanere

- AIDS trojaneren (1989)
 - Program som gav info om AIDS, men så krypterte filsystemet og tilbød nøkkelen mot en avgift
- Falsk antivirus
 - F.ex. XP Antivirus 2010, Mac Defender
 - Distribusjonsnettett tatt ned av Russiske myndigheter i Juni 2011
- Back Orifice (1998)
 - Distribuert pr epost, installerte en Win-service som åpnet remote pålogging

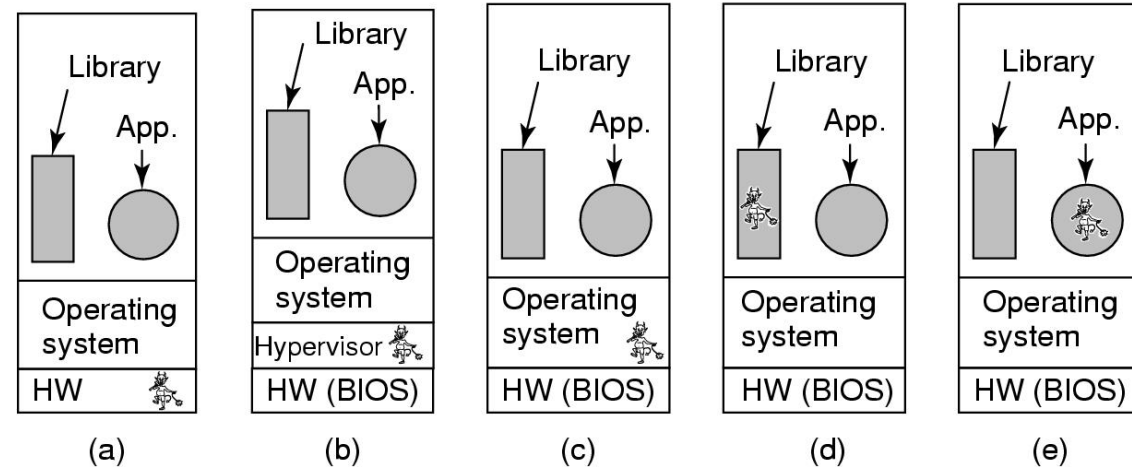
- Rootkit modifierer **OS** og **skjuler** sin eksistens
 - F.ex. Modifiserer filsystemets muligheter til å se en fil
 - Vanskelig å oppdage med programvare som jo er avhengig av OSet selv
- Sysinternals RootKitRevealer
 - Scanner hele filsystemet to ganger
 - **Høynivå** ved bruk av Windows API
 - Rå scan med disk-metoden
 - Ulikt resultat tyder på et rootkit
 - Virker dessverre bare på Windows XP...
- (Norman Intrusion Guard gjør det samme)

Rootkits

1. Firmware
2. Hypervisor
3. Kernel
4. Bibliotek
5. Applikasjon

Teknikker brukt av rootkits:

- Skjuling av prosesser/drivere
- Skjuling av registry oppføringer
- Skjuling av fysiske filer på disk

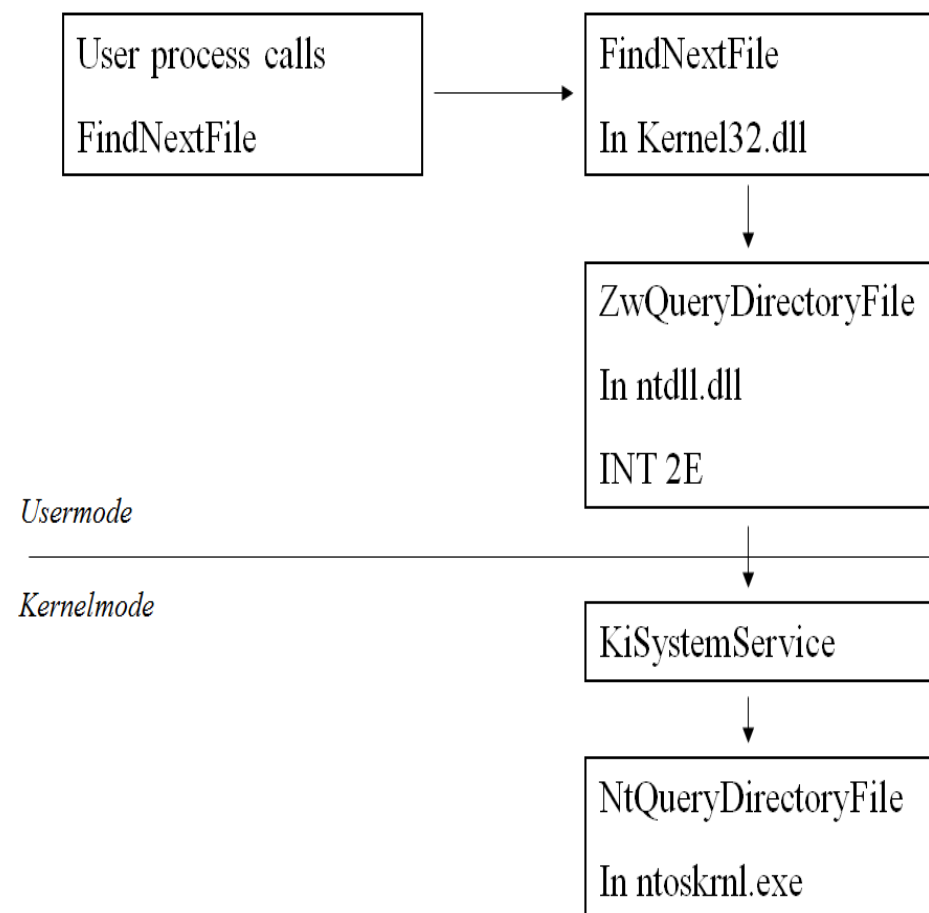


"Tidligere: Verktøy brukt av en hacker for å skaffe seg root access på en UNIX server. Inneholdt også ofte mulighet til å slette logger for å skjule spor etter hackingen."

"I dag: Egentlig ikke en egen type malware, men en teknikk brukt av malware for å skjule sine spor og gjøre seg selv usynlig på maskinen som er infisert."

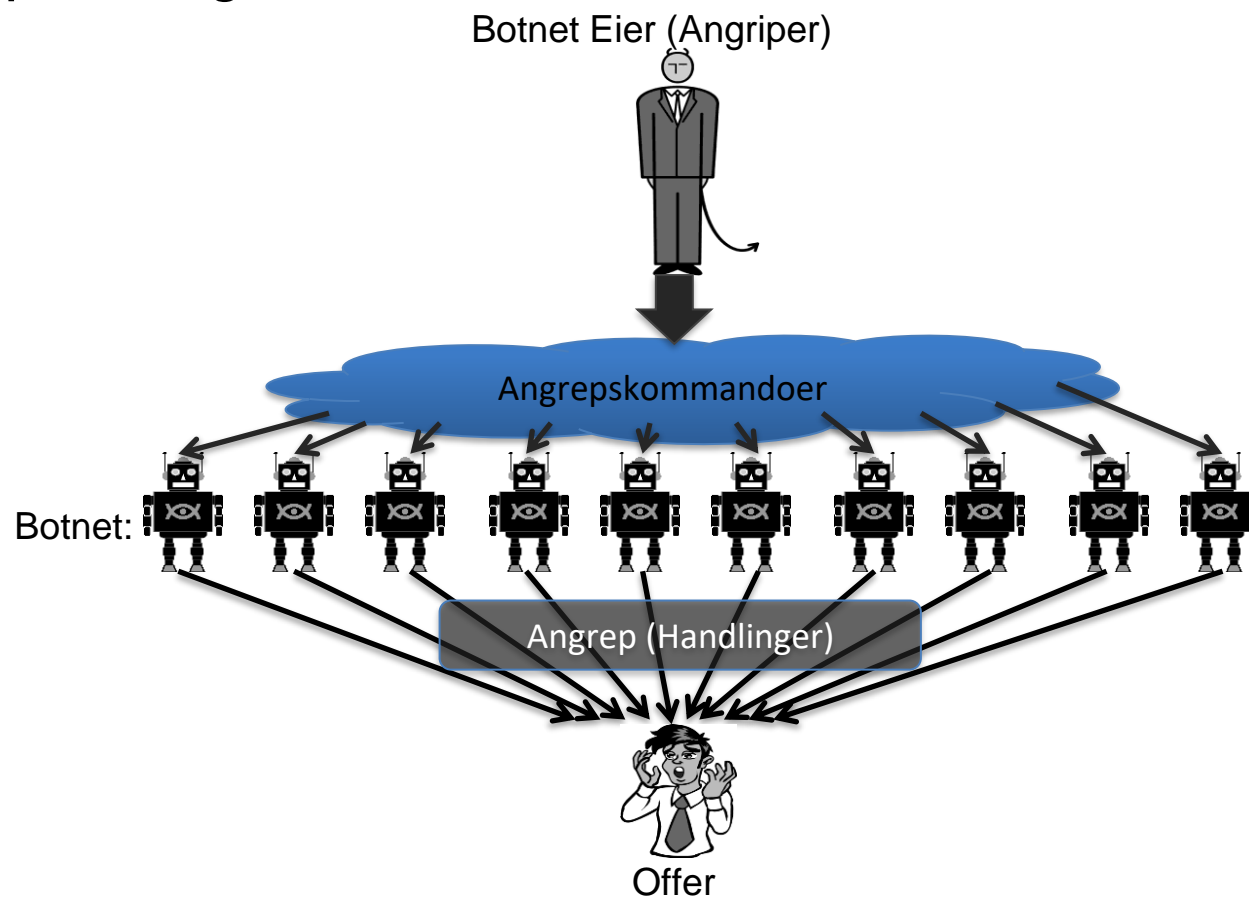
NT (Win32): Rootkit-eksempel

- Ved å hooke `NtQueryDirectoryFile` kan man velge å fjerne oppføringer av enkelte filer (som man ønsker å skjule).
- Dette vil da medføre at `FindNextFile` ikke viser filen du ønsker å skjule.
- Anti-Virus applikasjoner som skanner filer ved å enumerere ut filer på harddisken vil da ikke finne filen du har skjult.
- På denne måten har "rootkitten" klart å skjule seg selv på systemet.



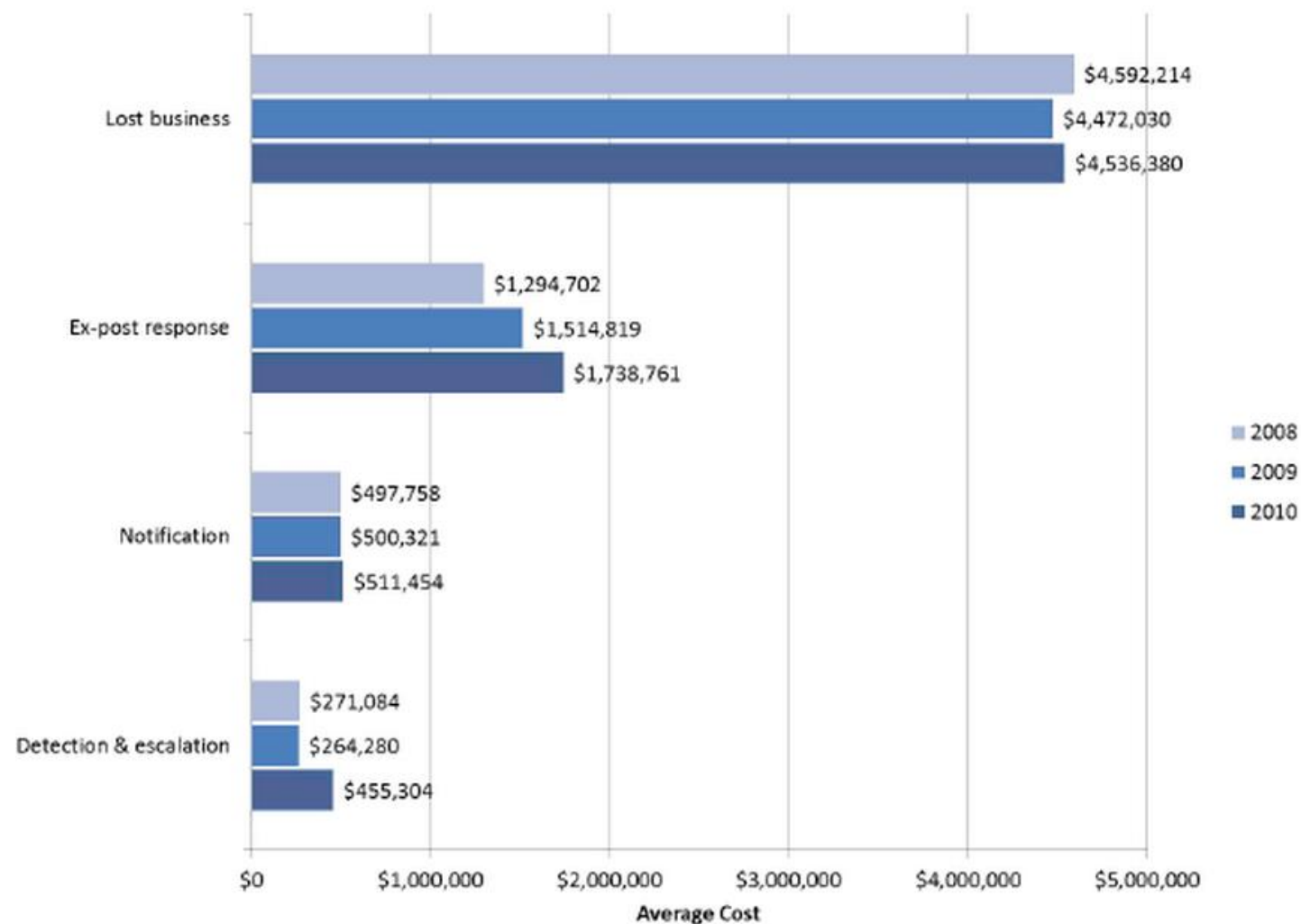
Malware Zombier (botnet)

- Malware kan gjøre en maskin om til en **zombie**, som er en eksternt kontrollert maskin som benyttes i ondsinnede angrep, vanligvis som del av et **botnet**



Økonomiske konsekvenser

- Malware påfører rammede firmaer tap og kostnader



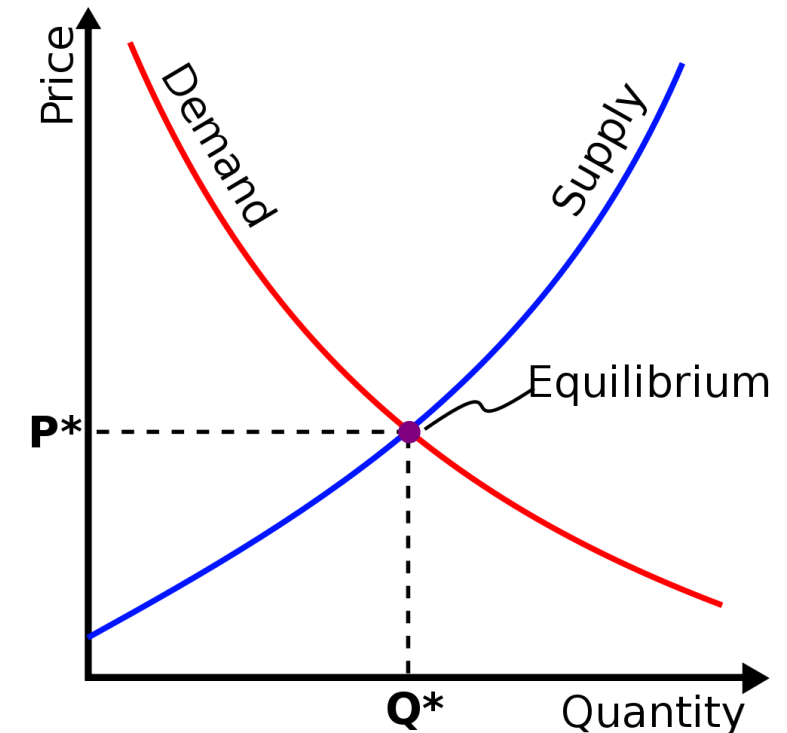
Kilde:
Ponemon
Institute:
[2010 Annual
Study:
U.S. Cost of a
Data Breach](#)

Eksempler på tap

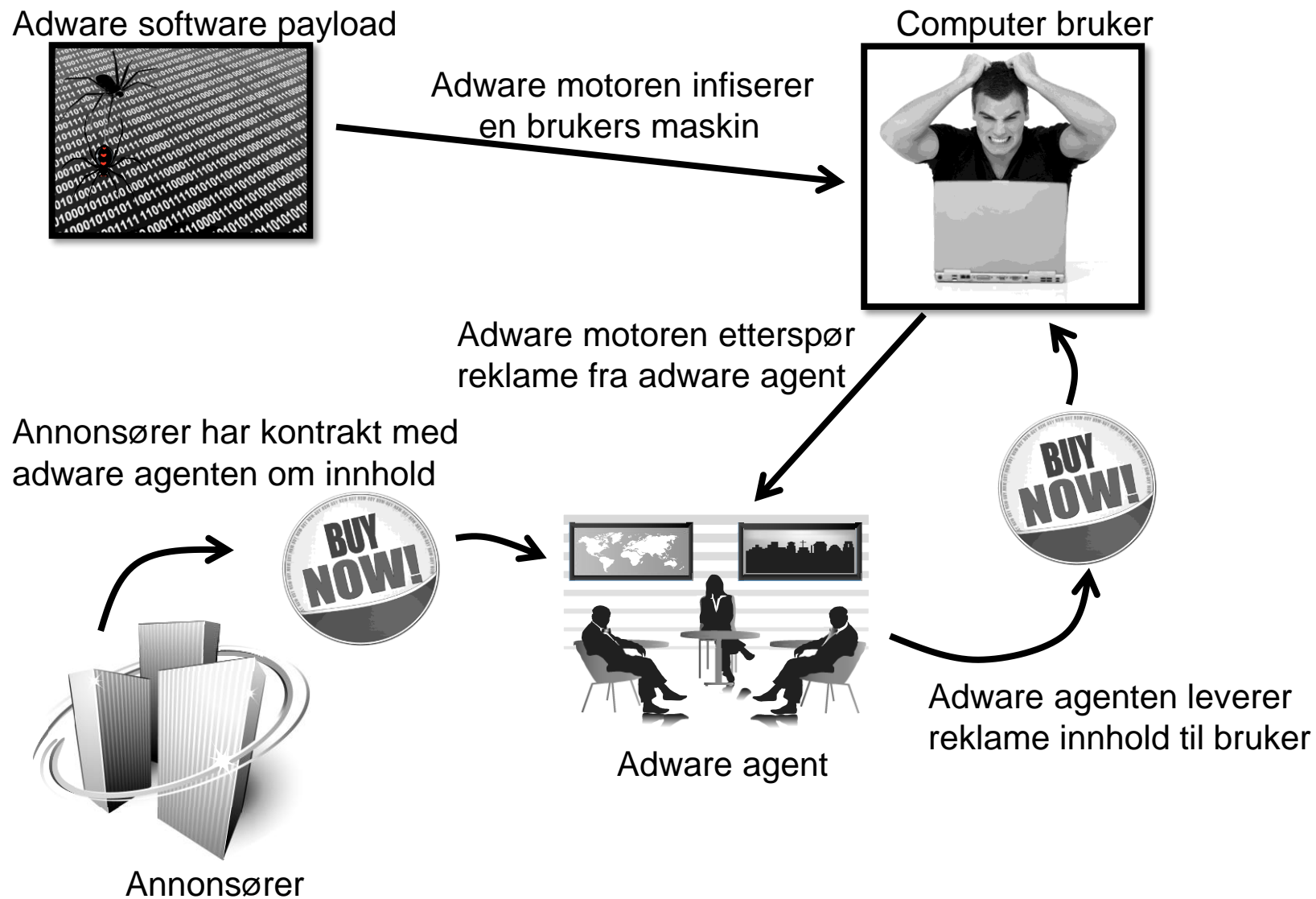
- Lovebug (2000)
 - Påførte tap på ca 8,5 billioner dollar og det Britiske parlamentet gikk ned
- W32.MyDoom.A (2008)
 - På toppen var 8% av alle eposter infisert
- Den russiske børsen gikk ned pga et virusangrep i 2006

Profesjonell malware

- Veksten i proff cyber-kriminalitet leder til en etterspørsel etter profesjonell malware
- Moderne malware er gjerne nye variasjoner av kjente angrep pakket i ulike produkter
- Følger loven om tilbud og etterspørsel
 - Botnet med 10000 bot'er ble tilbudt for \$15 i 2010
 - Keylogger fås for \$10
 - Zeus kommer raskt på \$500 (brukt), \$10000 (ferskt og nytt)

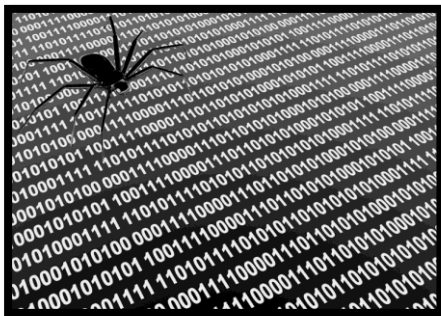


Adware



Spyware

Spyware programvare nyttelast



1. Spyware motor infiserer en brukers maskin.

Bruker



2. Spyware prosessen samler tastetrykk, passord, og skjermbilder.

3. Spyware prosessen sender periodisk samlede data til spyware data-innsamlingsagent.



Spyware datainnsamlings-agent

SpyEye

- I 2010 dukket SpyEye opp, et "klikk-og-dra" programmeringsverktøy for å lage malware som stjeler bankinformasjon.
- Det lages rettede angrep mot Nordea og DnB NOR
- Norske banker går ut i media februar 2011 og advarer kundene
- SpyEye koster 7000 kroner og selges til alle som ønsker å stjele bankinformasjon slik at disse kan lage trojanere uten særlig kunnskap...
- Til tross for høyt sikkerhetsnivå i norske banker ble flere svindlet
- Viktig årsak til at vi som kunder i dag må bruke to-faktor autentisering for hver betaling i nettbanken...

Anti-virus (AV)



Signaturer

- Scanning sammenligner det analyserte objektet med en database av **signaturer**
- En signatur er «fingeravtrykket» til et virus, eller annet stykke malware
 - M.a.o. en streng med sekvens instruksjoner som er spesifikke for hvert enkelt
 - Ikke det samme som en digital signatur
- En fil flagges som infisert dersom signaturen finnes inne i den
 - Rask **mønster-gjenkjenning** («pattern matching») teknikker benyttes for å søke etter signaturer
- Alle signaturene utgjør i felleskap en malware database som vanligvis er proprietær for produsenten av Anti-virus programvaren
- Signaturer beskytter kun mot malware som har blitt oppdaget og rapportert!

Navngiving

- Pr d.d. bruker ulike anti-virus leverandører ulike standarder for å navngi malware
- Oftest kommer malware i familier med betraktelige forskjeller mellom ulike generasjoner
- Noen benytter prefixer som
 - Win32 – Windows 32 bit API
- Noen benytter postfixer som
 - .A, .B – Variant/generasjon
 - @m – spres med epost
 - @mm – masse-epost utsender
- MAEC er (nok) et forsøk på å lage et standardisert språk for å karakterisere og beskrive malware ut fra adferd

- Mal/Conficker-A(Sophos)
- Win32/Conficker.A (CA)
- W32.Downadup (Symantec)
- W32/Downadup.A (F-Secure)
- Conficker.A (Panda)
- Net-Worm.Win32.Kido.bt (Kaspersky)
- W32/Conficker.worm (McAfee)
- Win32.Worm.Downadup.Gen (BitDefender)
- Win32:Confi (avast!)
- WORM_DOWNAD (Trend Micro)
- Worm.Downadup (ClamAV)

White/Black Listing

- Opprettholder en database med kryptografiske hash'er for
 - OS systemfiler
 - Vanlige applikasjoner
 - Kjente infeksjoner
- Beregn hash for hver fil dynamisk ved nedlasting, lasting og eksekveringsforsøk
- Slå opp i database
- Nekt/tillat ut fra resultat
 - Rapporter mistenkelig adferd til AV-leverandør
- Kan selvsagt selv infiseres og må beskyttes

Heuristisk analyse

- Brukes for å identifisere nye og «zero day» malware
- Kode analyse
 - Basert på instruksjonene forsøker AV å bestemme om det er malware ut fra at det f.ex. forsøker å endre/slette system-filer
- Emulering av eksekvering
 - Kjøre koden i isolert miljø («sandbox»)
 - Overvåk adferden
 - Dersom mistenkelig adferd -> marker som malware
- Kan automatiseres, men utløse falske alarmer

Statisk vs dynamisk analyse

Statisk

- Sjekker koden uten å prøve å eksekvere den
- Sjekk mot White list
- Filtrer og fjern alt korrekt i filen for å forsøke å isolere ut virus
- Sjekk binær kode for å finne filtype
- Undersøk binære instruksjoner og data

Dynamisk

- Undersøk eksekveringen av koden i en virtuell sandkasse
- Monitorer
 - Fil-endringer
 - Registry-endringer
 - Prosesser og tråder
 - Nettverks-porter

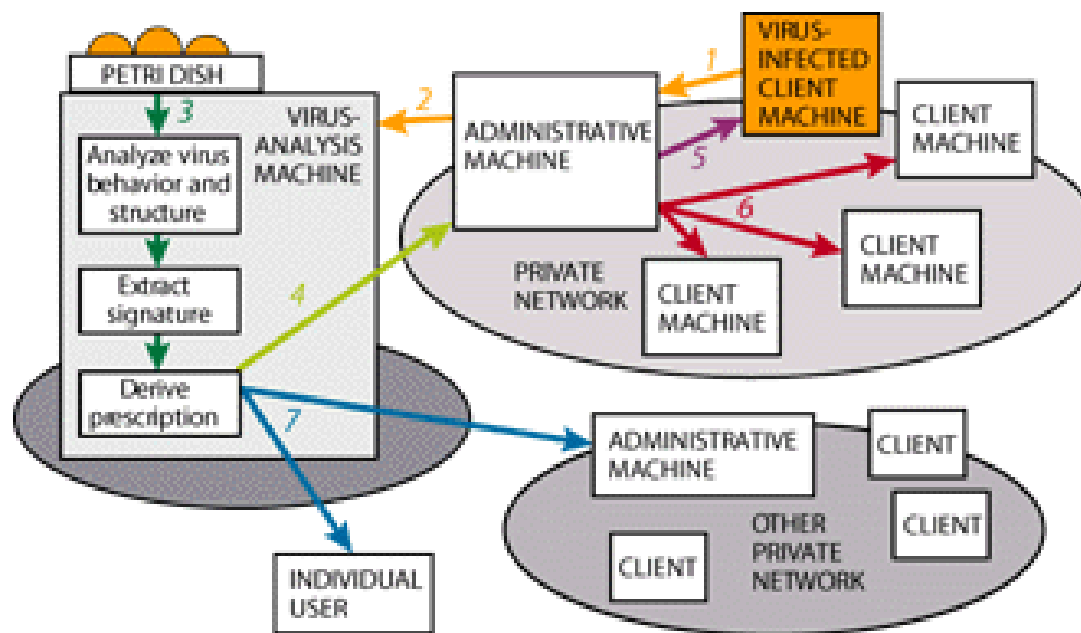
- En mistenkelig fil kan isoleres i en **egen katalog** og settes i karantene
 - Det vanlige er at alle infeksjoner karantineres, da det kan være en falsk positiv (eller bruker vil kanskje ha dokumentet – selv om det er infisert...)
- Den mistenkelige filen slettes ikke, men **ufarliggjøres**
 - Brukeren kan selv velge om den skal fjernes, eller gjenopprettes
 - Interaksjon med filen skal kun være mulig gjennom AV-programmet
- Filer i karantene er harmløse fordi de blir **kryptert**
- Ulike AV gjør dette på ulike måter og hemmeligholder teknikkene...

Digitale immunsystemer

- Moderne anti-virus forsøker å tilby et fullstendig «immunsystem» der mistenkelige filer og adferd rapporteres, overføres til analyse og signaturer oppdateres
- F.ex. MS SpyNet i MS Security Essentials

collected and sent.

- ☐ I do not want to join SpyNet
No information will be sent to Microsoft if a virus is detected running on your computer.
- ☒ Basic membership
Send basic information to Microsoft including where the software is running. Microsoft Security Essentials applies automatic updates. Microsoft will not use this information for anything other than security purposes.
- ☐ Advanced membership
In addition to basic information, Microsoft will also receive information about how the software is running, how it has impacted your computer, and how it has impacted your network. This information is sent to Microsoft to help identify you or contact you.

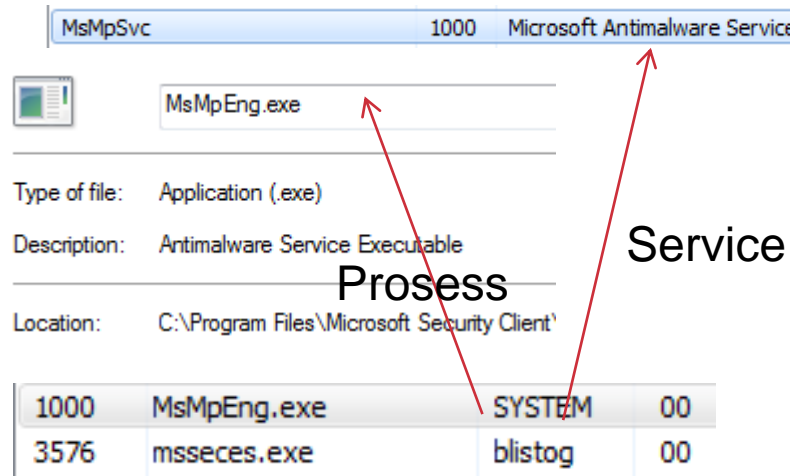


Kilde: <http://goo.gl/gb6xz>

Ved-tilgang vs Ved-behov

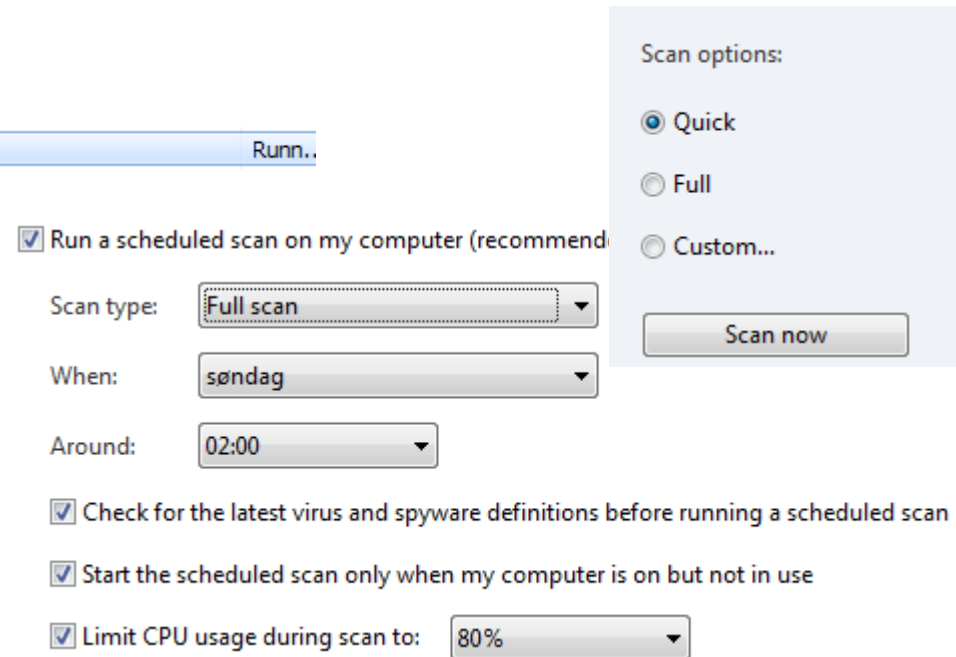
• On-access

- Kalles av noen for Shield
- Bakgrunnsprosess
 - Service/daemon
- Scanner hver gang en fil blir brukt (open, copy, execute, osv)



• On-demand

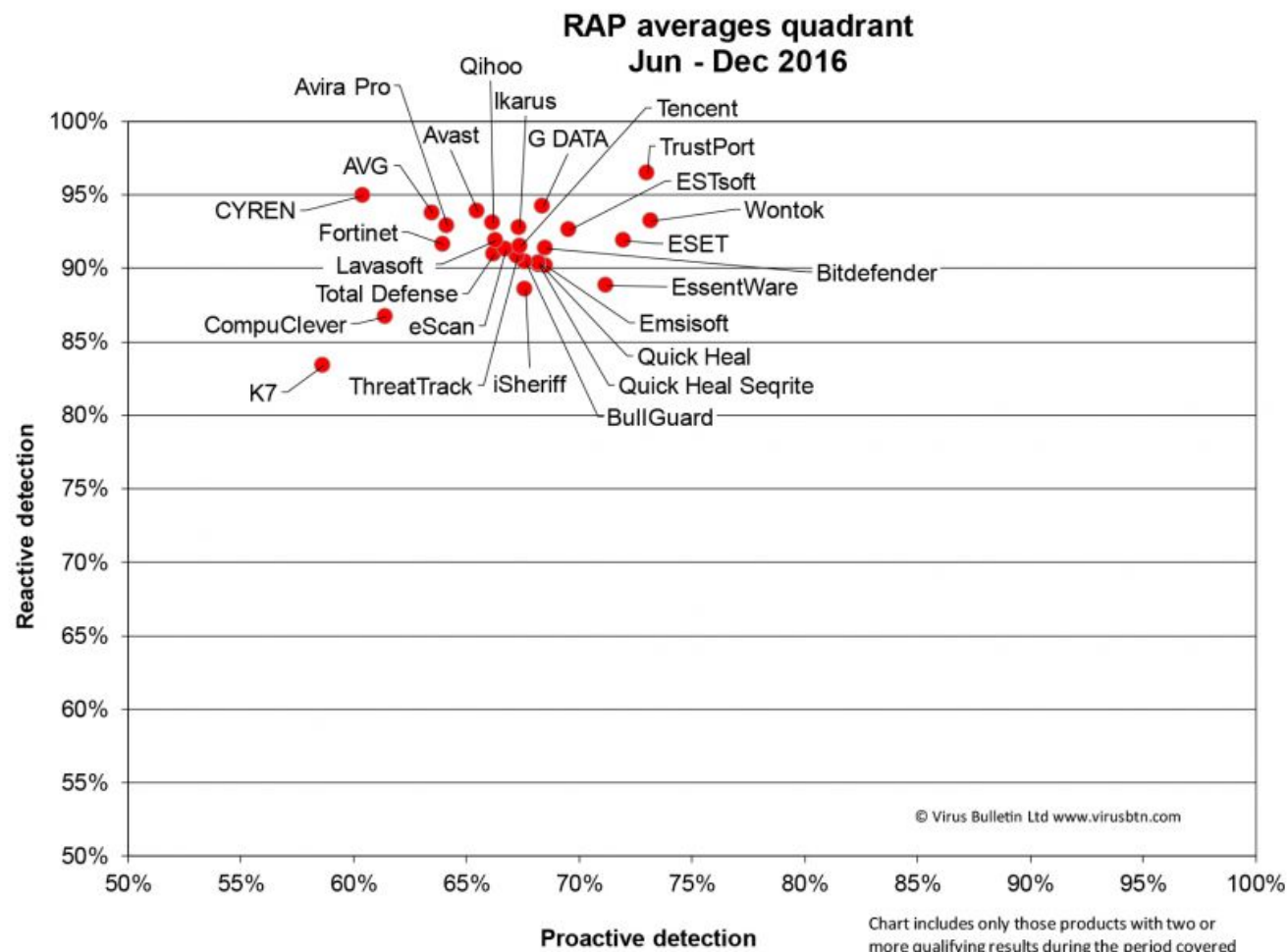
- Scan ut fra etterspørsel
 - fra bruker,
 - eller periodisk
- På mistenkelig/ny fil, katalog, e.l.



Tester av anti-malware

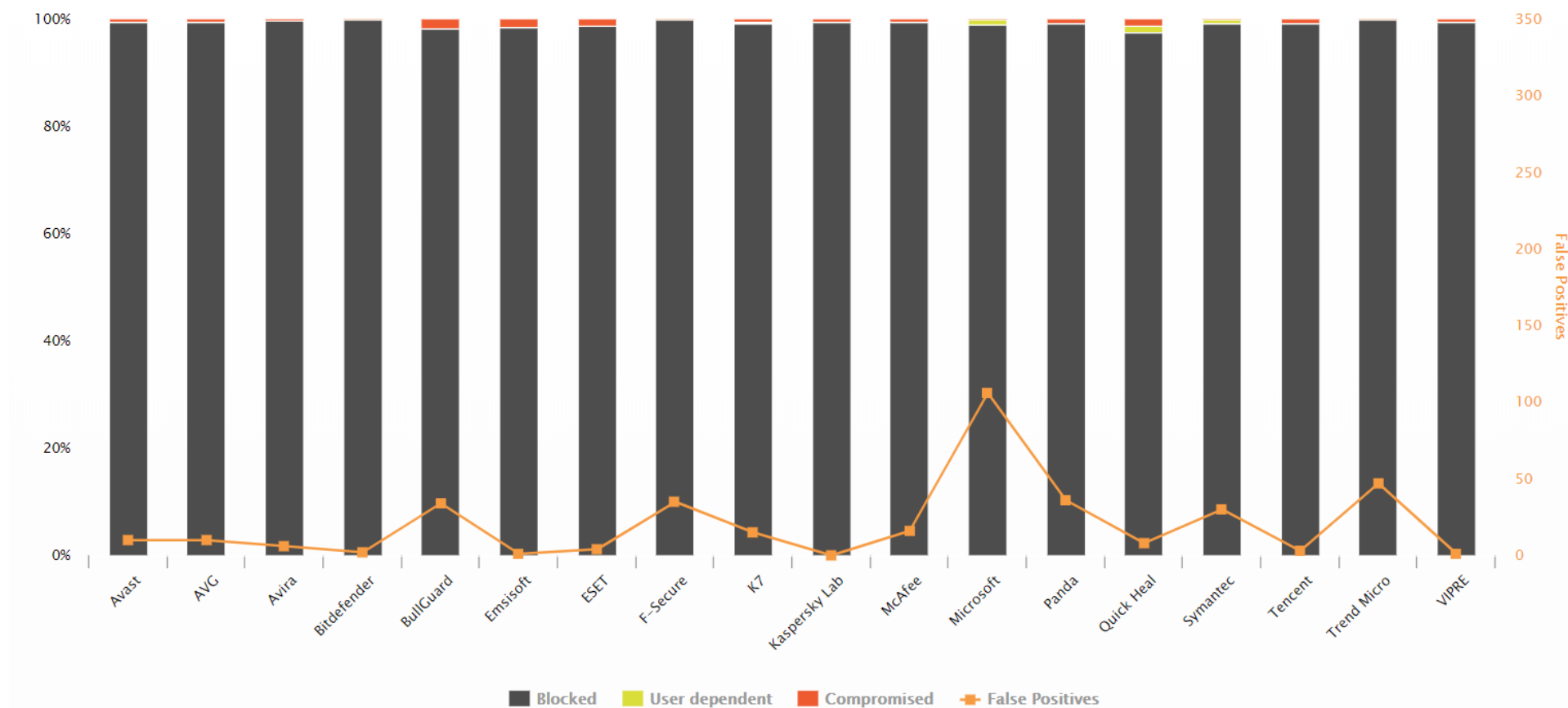
- AV testes bl.a. ut fra hvor gode scanning-teknikkene deres er
 - Komparativt
 - Sjekker antall allerede kjente malware og signaturer som blir funnet og hvor lang tid det tar
 - Retrospektiv
 - Test proaktiv evne til å mistenke ukjent malware
 - Sjekker effektiviteten til heuristikken
- Er på papiret uavhengige, men de selger ofte tjenester og har derfor visse økonomiske incentiver...

Virus Bulletin



<https://www.virusbulletin.com/testing/dates/vb100-antimalware>

AV Comparatives



<https://chart.av-comparatives.org/chart1.php>

AV-TEST

August 2016

	Name		Protection	Performance	Usability	remove
AhnLab	AhnLab V3 Internet Security 9.0					
avast	Avast Free AntiVirus 2016					
AVG	AVG Internet Security 2016					
Avira	Avira Antivirus Pro 2016					
Bitdefender	Bitdefender Internet Security 2016					
BullGuard	BullGuard Internet Security 16.0					
Check Point	Check Point ZoneAlarm Extreme Security 14.2 &...					
Comodo	Comodo Internet Security Premium 8.4					
Emsisoft	Emsisoft Anti-Malware 11.9 & 11.10					
ESET	ESET Smart Security 9.0					
F-Secure	F-Secure Safe 2016					
G Data	G Data InternetSecurity 2016					
K7 Computing	K7 Computing Total Security 15.1					
Kaspersky Lab	Kaspersky Lab Internet Security 2017					

<https://www.av-test.org/en/compare-manufacturer-results/>

Online vs Off-line

Online

- Gratis
- Browser plug-in
- MÅ være digitalt signert (ellers= scam)
- Ingen on-access scanning
- Alltid oppdaterte signaturer
- Lite konfigurerbart
- Krever Internett-forbindelse
- Data samles inn av firmaet som tilbyr tjenesten
- Anbefales egentlig ikke...

Off-line

- Oftest abonnement
- Installerer i OS
- Må distribueres sikkert online eller fra utsalg
- System skjold
- Må selv velge frekvens for oppdateringer av signaturer og software
- Lett konfigurerbart
- Kan scanne uten internett-forbindelse
- Rapporter til firma-portal lokalt, eller sendes leverandør

Et botnet-eksempel

Selv om Malware er skummelt er det viktig å være oppmerksom på at:

*Moderne malware kommer (hovedsakelig) som **pakker** spredd på WWW!*

Eksempel: Blackhole

- Du kjøper en ferdig server-løsning av Blackhole-rammeverket

Annual license: \$ 1500

Half-year license: \$ 1000

3-month license: \$ 700

Update cryptor \$ 50

Changing domain \$ 20 multidomain \$ 200 to license.

During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): \$ 200

2 weeks (14 full days): \$ 300

3 weeks (21 full day): \$ 400

4 weeks (31 full day): \$ 500

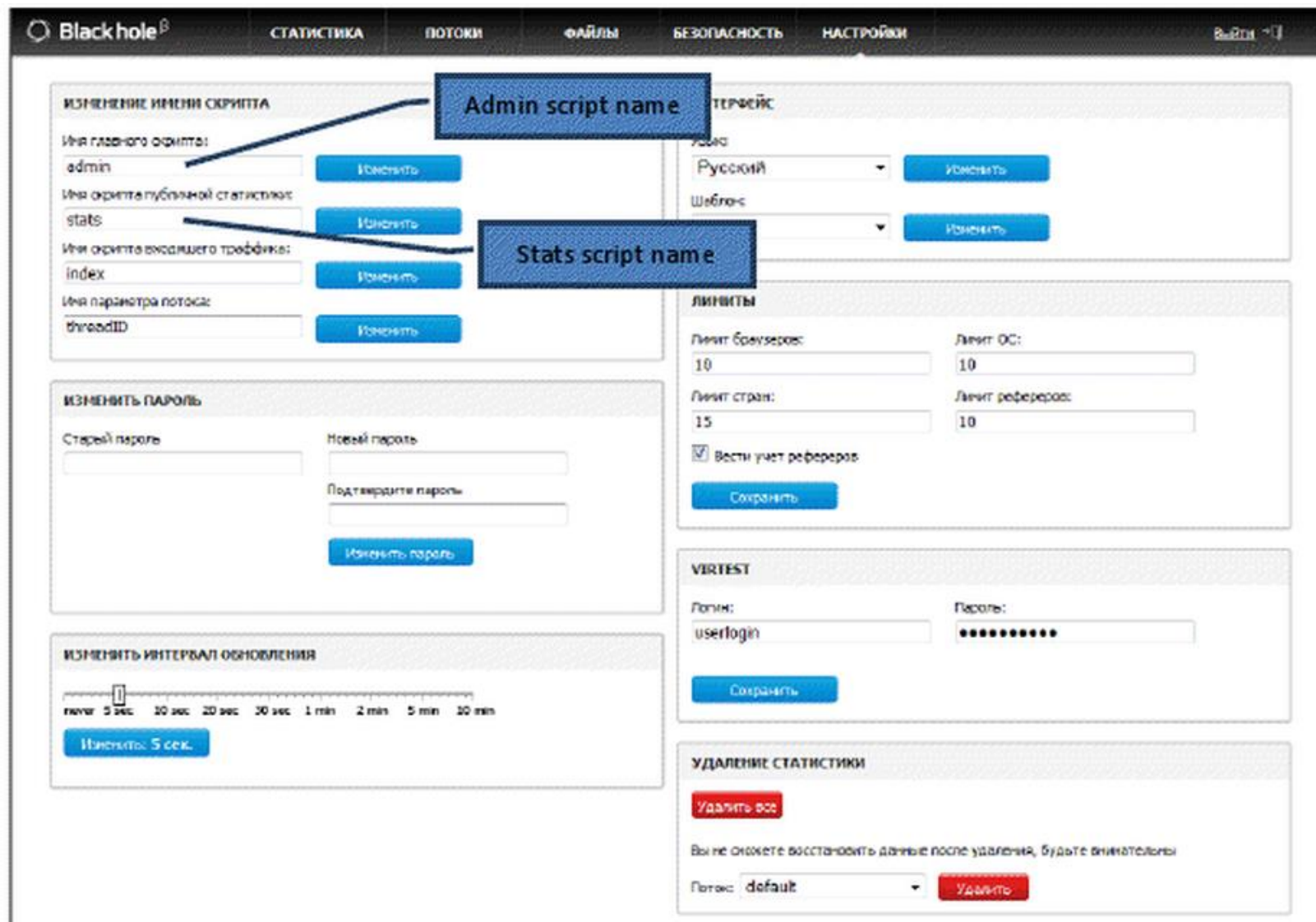
24-hour test: \$ 50

There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: \$ 35

No longer any hidden fees, rental includes full support for the duration of the contract.

BlackHole: GUI for admin



The screenshot shows the BlackHole administration interface. At the top is a navigation bar with tabs: **СТАТИСТИКА**, **ПОТОКИ**, **ФАЙЛЫ**, **БЕЗОПАСНОСТЬ**, and **НАСТРОЙКИ**. The **НАСТРОЙКИ** (Settings) tab is active. The interface is divided into several sections:

- ИЗМЕНЕНИЕ ИМЕНИ СКРИПТА** (Change script name): This section contains four rows, each with a text input field and a blue **Изменить** (Change) button. The first row is for the main script name, currently set to `admin`. A blue callout box labeled **Admin script name** points to this field. The second row is for the public statistics script name, currently set to `stats`. A blue callout box labeled **Stats script name** points to this field. The third row is for the outgoing traffic script name, currently set to `index`. The fourth row is for the stream parameter, currently set to `threadID`.
- ИЗМЕНИТЬ ПАРОЛЬ** (Change password): This section has three input fields: **Старый пароль** (Old password), **Новый пароль** (New password), and **Подтвердите пароль** (Confirm password). A blue **Изменить пароль** (Change password) button is at the bottom.
- ИЗМЕНИТЬ ИНТЕРВАЛ ОБНОВЛЕНИЯ** (Change update interval): This section features a slider ranging from **5 сек.** to **30 мин.**. The current value is set to **5 сек.**, with a blue **Изменить: 5 сек.** (Change: 5 sec.) button below it.
- ТЕРМЯЙС** (Interface): This section includes a **Язык** (Language) dropdown menu set to **Русский** and a **Шаблон** (Template) dropdown menu. Both have blue **Изменить** (Change) buttons.
- ЛИМИТЫ** (Limits): This section contains four input fields for limits: **Лимит браузеров** (10), **Лимит ОС** (10), **Лимит стран** (15), and **Лимит рефереров** (10). There is a checked checkbox for **Вести учет рефереров** (Track referrers) and a blue **Сохранить** (Save) button.
- VRTTEST**: This section has **Логин** (Login) set to `userlogin` and a **Пароль** (Password) field masked with dots. A blue **Сохранить** (Save) button is at the bottom.
- УДАЛЕНИЕ СТАТИСТИКИ** (Delete statistics): This section has a red **Удалить все** (Delete all) button. Below it is a warning message: **Вы не сможете восстановить данные после удаления, будьте внимательны** (You cannot restore data after deletion, be careful). At the bottom, there is a **Поток** (Stream) dropdown menu set to `default` and a red **Удалить** (Delete) button.

BlackHole: Payload

- Sjekker med Javascript hvilken pakke som skal leveres ut fra identifisert svakhet i OS, browser/plugin
- Sjekker med Javascript
- Leveres med epost-link eller XSS.

Exploit delivered	Vista: IE7, IE8 Win7: IE9, IE10	Win7: Mozilla22, Opera12, Safari5 Android: Safari5	Win7: Firefox14	Vista: IE6	Non-Windows platforms	WinNT90: IE9	Win8: Chrome17
Java (CVE-2010-0840, CVE-2012-0507)	+	+	+	+	-	+	+
XMLHTTP+ADODBSTREAM downloader (MS06-014)	-	-	-	+	-	-	-
(CVE-2009-0927, CVE-2008-2992, CVE-2009-4324, CVE-2007-5659) or CVE-2010-0188	+(IFRAME)	+(object)	+(IFRAME + object)	+(IFRAME)	-	+(IFRAME)	+(object)
HCP (CVE-2010-1885) XMLHTTP+ADODB	-	-	-	-	-	-	-
Flash (CVE-2011-0611)	-	-	-	-	+	+	+
Flash (CVE-2011-2110)	+	+	+	+	+	+	+
CVE-2012-1889	-	-	-	-	-	-	-

BlackHole: Payload

- Typisk stjele passord, og click-jacking

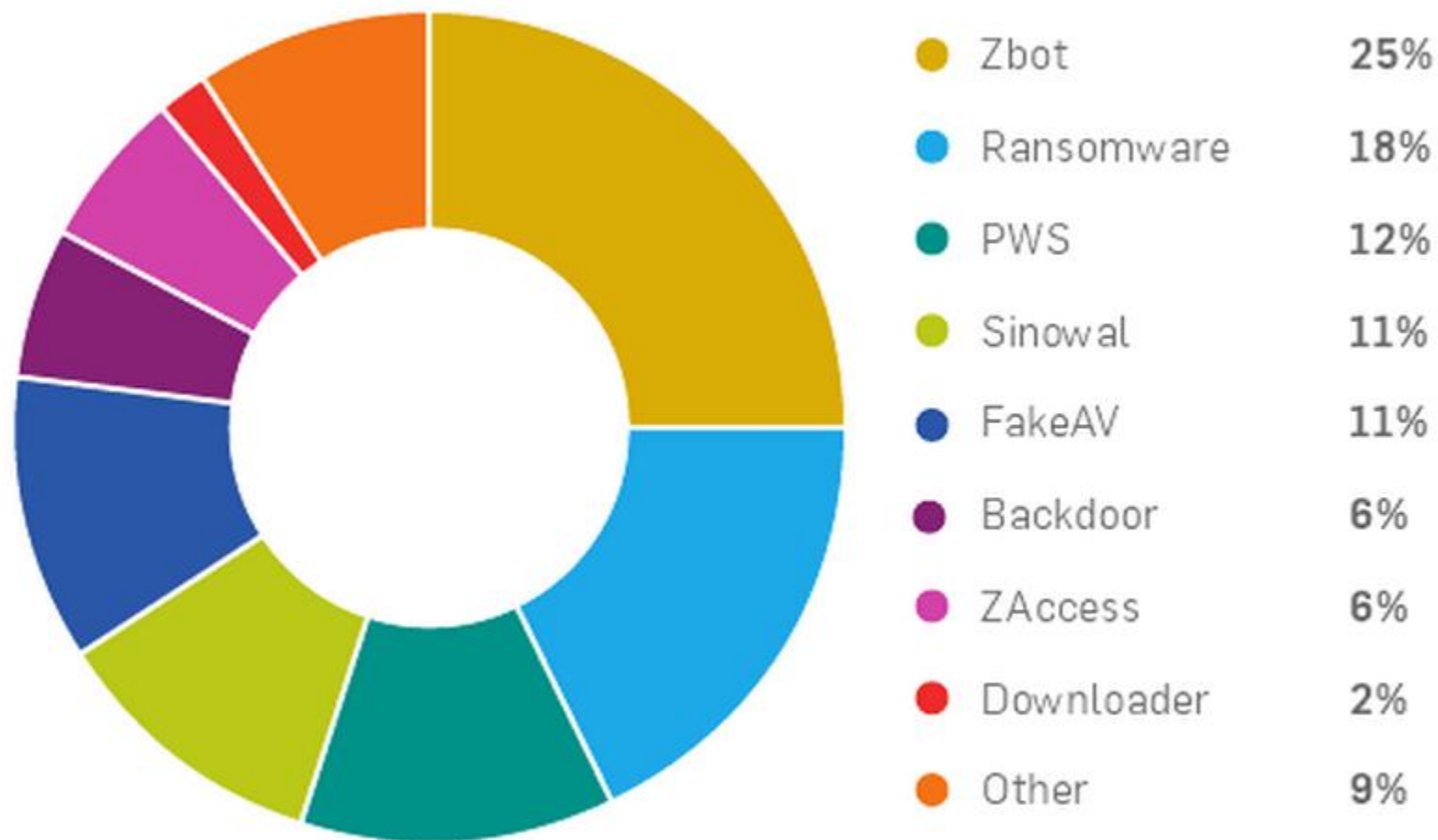


fig. 23: Payload breakdown

OPPSUMMERING

Hva skal vi kunne

- Definisjonene av de ulike **typene malware**
 - Hvordan de spres
 - Hvordan de skjuler seg
 - Hva som er målet med dem
- **Anti-virus**
 - Hva programvaren kan «se etter»
 - Signatur
 - Adferd
- **MEN:** moderne malware kommer (hovedsakelig) som **pakker** spredd på WWW!

Praktisk laboppgave anti-virus #1

1. Har du installert anti-virus programvare (Windows Defender teller ikke...)

Hvis ikke; last ned 90 dager gratis trial av Bitdefender Total Security

<https://www.bitdefender.com/media/html/consumer/new/get-your-90-day-trial-opt/index.html>

2. Gå på www.av-test.org og se hvordan din anti-virus programvare har gjort det i tester.

3. Gjør deg kjent med bruker interface, finn følgende;

Karanteneinnstillinger og filer

Opsjon for å skru av real-time beskyttelse

Brannmur innstillinger og regler

Praktisk laboppgave anti-virus #2

4. Åpne en tekst-editor

5. Legg inn:

```
X5O!P%@AP[4\PZX54(P^) 7CC) 7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

6. Lagre som `mittvirus.com`

7. Gjør det samme og
lagre som `mittvirus.txt`

Hva betyr det hvis oppførselen er forskjellig? (Hint; noen anti-virus program søker faktisk ikke i alle filer...)



Praktisk laboppgave anti-virus #3

8. Skru av real-time beskyttelse
9. Opprett mittvirus.com (se oppgave 5)
10. Legg mittvirus.com inn i en ZIP fil mittvirus.zip
11. Legg mittvirus.com inn i en kryptert ZIP fil emittvirus.zip
12. Skru på real-time beskyttelse
13. Kopier filene – blir de slettet av anti-virus? (real-time)
14. Åpne filene – blir de slettet av anti-virus?
15. Pakk ut innholdet i filene – blir de slettet av anti-virus?
16. Høyre klikk på filene og velg å søke etter virus...

DATAVIRUS MED KINETISK UTFALL...