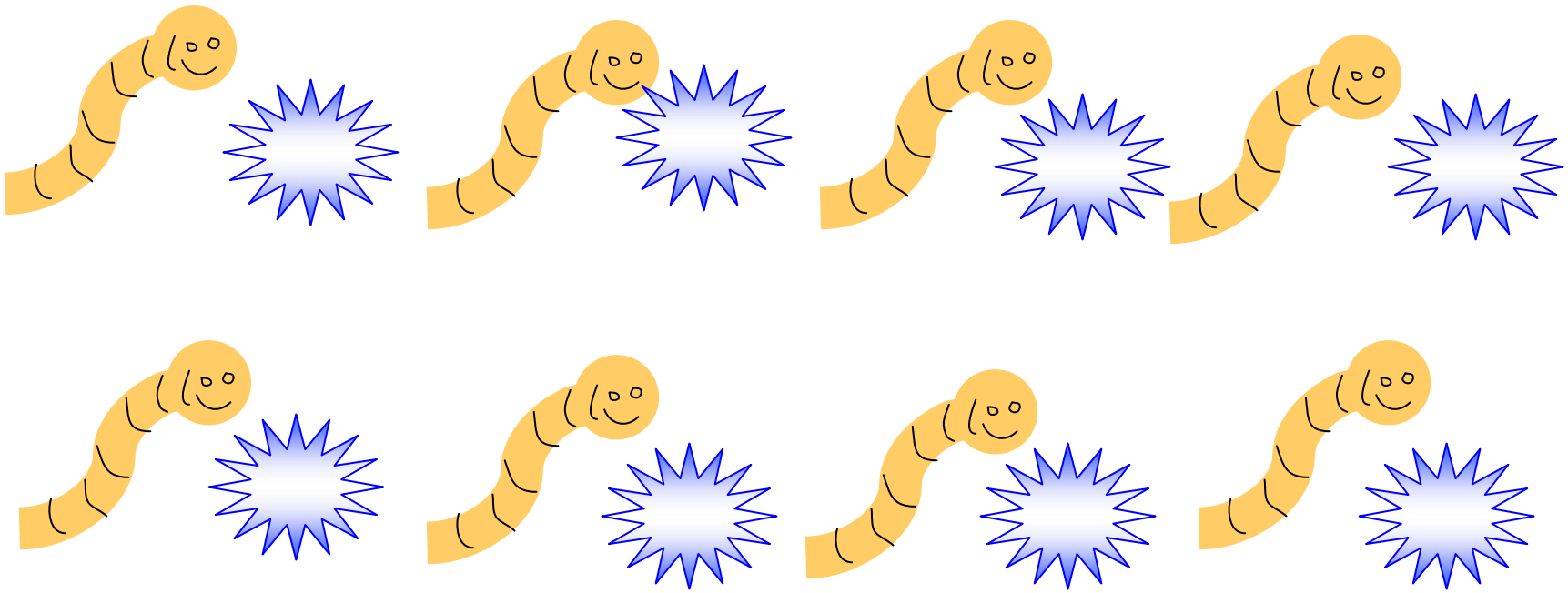
Aktualni virusni rizici

Najčešći virusi u 2000. godini

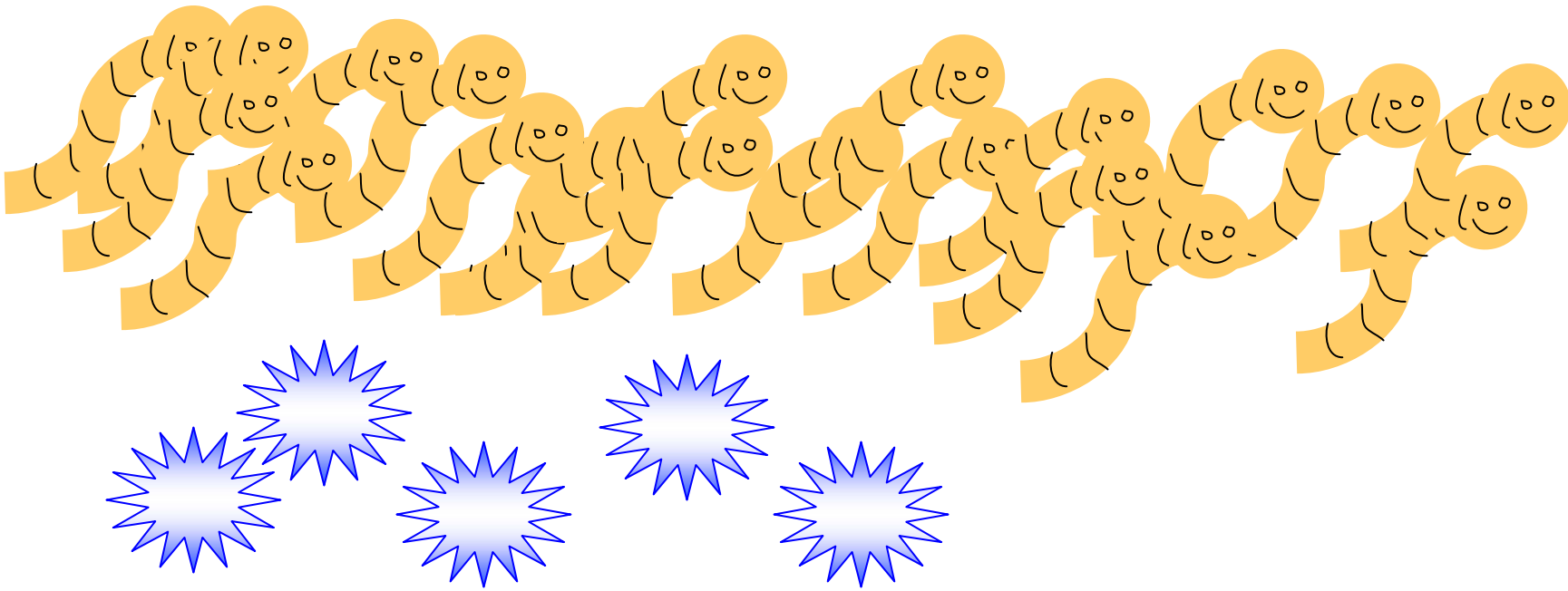
- Najčešći virusi u 2000. godini su zapravo crvi
- Automatska distribucija povećava šanse za preživljavanje
- Najčešće korištene aplikacije su pogodna podloga

Crvi i virusi među korisnicima – broj



Danas među korisnicima *(in the wild)*
crvi i virusi nalaze se u istom broju

Crvi i virusi među korisnicima – infekcije



Ali crvi su neusporedivo infektivniji.

Noviji virusi među korisnicima

- Virus W32/Apology
- Crv W32/Hybris
- Crv VBS/Kakworm
- Crv W32/Navidad-B (Emanuel)

Crv W32/Apology

- Kolovoz 2000.
- 32 različita naziva datoteke u dodatku
- Windows 32 bitni EXE
- Mijenja WSOCK32.DLL
- Svaku poslanu poruku slijedi inficirana

Crv W32/Apology – nazivi datoteka

README.TXT.pif
I_wanna_see_YOU.TXT.pif
MATRiX_Screen_Saver.SCR
LOVE_LETTER_FOR_YOU.TXT.pif
NEW_playboy_Screen_saver.SCR
BILL_GATES_PIECE.JPG.pif
TIAZINHA.JPG.pif
FEITICEIRA_NUA.JPG.pif
Geocities_Free_sites.TXT.pif
NEW_NAPSTER_site.TXT.pif
METALLICA_SONG.MP3.pif
ANTI_CIH.EXE
INTERNET_SECURITY_FORUM.DOC.pif
ALANIS_Screen_Saver.SCR
READER_DIGEST_LETTER.TXT.pif
WIN_$100_NOW.DOC.pif
IS_LINUX_GOOD_ENOUGH!.TXT.pif
QI_TEST.EXE
AVP_Updates.EXE
SEICHO-NO-IE.EXE
YOU_are_FAT!.TXT.pif
FREE_xxx_sites.TXT.pif
I_am_sorry.DOC.pif
Me_nude.AVI.pif
Sorry_a bout_yesterday.DOC.pif
Protect_your_credit.HTML.pif
JIMI_HMNDRIX.MP3.pif
HANSON.SCR
FUCKING_WITH_DOGS.SCR
MATRiX_2_is_OUT.SCR
zipped_files.EXE
BLINK_182.MP3.pif

Crv W32/Hybris

- Studeni 2000.
- Randomski nazivi dodatka
- Windows 32 bitni EXE
- Crv se može automatski dograđivati
- Brojne varijante
- Anonimne poruke

Crvi W32/Navidad i W32/Navidad-B

- Studeni 2000.
- Windows 32 bitni EXE
- Ne funkcionira ispravno
- Masovno slanje poruka
- Pogođeni kompjuter “neupotrebljiv”
- Uklanja se trikom

Crv VBS/Kakworm

- Siječanj 2000.
- Varijante veljača i srpanj 2000.
- “Kagou-Anti_Kro$oft says not today”
- **Nema *attachmenta* – crv je u poruci!**
- Koristi bug (MS IE 4.0 i 5.0) tzv. *ActiveX scriptlet.typelib* i *Eyedog vunerability* (VBS/BubbleBoy)

Crv VBS/Kakworm

- Možete imati AV program i dalje biti inficirani, bez obzira što vaš AV program prepoznaje VBS/Kakworm
- Ako instalirate *patch* ili koristite MS IE 5.01 ili 5.5 ne možete biti inficirani bez obzira da li vaš AV program uopće prepoznaje virus
- **KORISTITE *PATCHEVE*!!!**

Hoax (“patka”, šala, prijevara)

- Socijalni inženjering
- Prijetnja malicioznim sadržajem (najčešće virusom) i usporedba tipa “jači od Melisse”
- Poziv na autoritet (IBM, AOL, Microsoft)
- Uputa da se proslijedi svim prijateljima ili svima čiji e-mail imate

Hoax (“patka”, šala, prijevara)

Vi potpisujete (potvrđujete) laž!

Hoax (“patka”, šala, prijevara)

- Lukavi trikovi
- Sažaljenje
- Nagradne igre (Nokia GSM)
- Pohlepa
- Ljubavne ponude
- Ne biste vjerovali tko sve nasjeda :-)

Hoax (“patka”, šala, prijevara)

- Ne prosljeđivati *(delete)*
- Ako odgovarate pošiljatelju – kratko, jasno i uključite *hoax* info URL
- Informirajte korisnike, i uputite ih da ne prosljeđuju razna upozorenja *(hoax)*
- U AV industriji nezatražena upozorenja ne postoje

Što možete naći na Internetu?

- Antivirusne programe i dogradnje
- Informacije o malicioznom softveru
- Informacije o lažnim uzbunama *(hoax)*
- Informacije o greškama i drugim sigurnosnim rizicima
- Ispravke programa *(patch)*

Korisne web adrese

- Sophos Plc
  - www.sophos.com/virusinfo
  - **www.sophos.com/virusinfo/notifications**
  - www.sophos.com/virusinfo/analyses
  - **www.sophos.com/virusinfo/hoaxes**
- **www.qubis.hr**

Qubis – informacije o virusima

- www.qubis.hr/apology
- www.qubis.hr/hybris
- www.qubis.hr/kakworm
- www.qubis.hr/navidad
- www.qubis.hr/savjeti
- www.qubis.hr/hoax

Korisne web adrese

- CERT *(Computer Emergency Response Team)*
  - www.cert.org
  - www.cert.org/contact_cert/certmaillist.html

Korisne web adrese

- Microsoft Corporation
  - http://windowsupdate.microsoft.com/
  - http://officeupdate.microsoft.com/