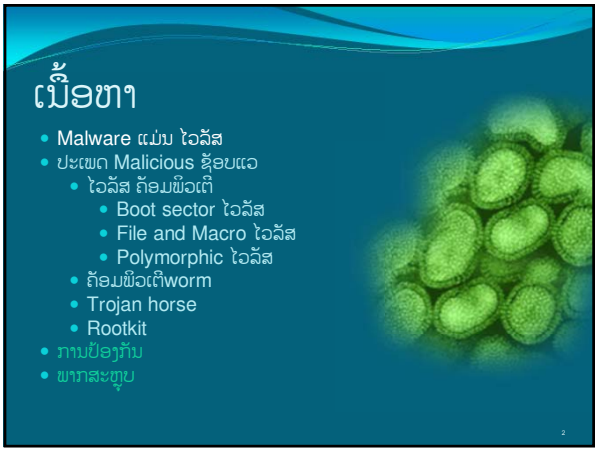

ການປ້ອງກັນ ໄວລັສ ແລະ
Malware
ໂດຍ: ຄະຈອນສັກ
ວັນພຸດທີ 29 ສິງຫາ 2012


ເນື້ອຫາ
Malware ແມ່ນ ໄວລັສ
ປະເພດ Malicious ຊ໊ອບແວ
ໄວລັສ ຄ້ອມພິວເຕ້
Boot sector ໄວລັສ
File and Macro ໄວລັສ
Polymorphic ໄວລັສ
ຄ້ອມພິວເຕ້worm
Trojan horse
Rootkit
ການປ້ອງກັນ
ພາກສະຫຼຸບ

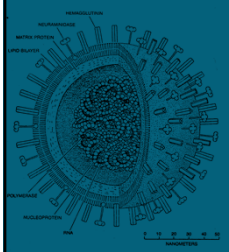

Malware ແມ່ນ ໄວລັສ
ໄວລັສ ຄ້ອມພິວເຕ້ ແລະ Malware – Malicious Software ແມ່ນໃຊ້ສິບສົນກັນ
Malware ແມ່ນຖືກອອກແບບມາໃຫ້ ທຳການລົບກວນການ ທຳງານ ຂອງຄ້ອມພິວເຕ້, ທຳການຮວມຮວມຂໍ້ມູນຂອງຜູ້ໃຊ້ເຮັດໃຫ້ມີການສູນເສຍຂໍ້ ມູນ ແລະ ການນຳໃຊ້ຂໍ້ມູນໃນທາງທີ່ບໍ່ເໝາະສົມ, ສາມາດບຸກລຸກຄ້ອມພິວເຕ້ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ, ແລະ ການບຸກລຸກຕ່າງໆ
Malware ລວມມີ worms, Trojan horses, rootkits, spyware, adware ແລະ ຊ໊ອບແວທີ່ບໍ່ຕ້ອງການ ອື່ນໆ.

ປະເພດ Malicious software types

- ໄວລັສ Computer
- ຄ້ອມພິວເຕີ worm
- Trojan horse
- Rootkit
- Spyware
- Dishonest adware

4

ໄວລັສ Computer



- ໄວລັສ Computer ເປັນໂປຣແກຼມ ທີ່ສາມາດ ກ໊ອບປີ້ຕົວເອງ ແລະ ຕິດເຊື້ອໃຫ້ຄ້ອມພິວເຕີ
- ເພື່ອທີ່ຈະສາມາດກ໊ອບປີ້ຕົນເອງໄດ້, ໄວລັສຕ້ອງ ມີການໃຫ້ອະນຸຍາດໃຫ້ມີການມີການ execute code ແລະ ຂຽນລົງ memory
- ໄວລັສທົ່ວໄປລວມມີ: ໄວລັສ Boot sector , File ໄວລັສ , Macro ໄວລັສ ແລະ ໄວລັສ Polymorphic

5

ໄວລັສ Boot Sector

- Boot sector ຫຼື Master boot record, ແມ່ນເປັນ ພາກສ່ວນທຳອິດໃນຮາດດິສ, ເມໂມລີ ສະຕິກ ຫຼື ອຸປະກອນ ພາຍນອກທີ່ສາມາດບັນທຶກໄດ້ອື່ນໆ.
- ພາກສ່ວນທຳອິດ ແມ່ນເປັນພາກສ່ວນທີ່ເຂົ້າໄດ້ກ່ອນໝຸ່ງ.
- ໄວລັສ boot sector ແມ່ນຖືກອອກແບບມາໂຈມຕີຕໍ່ພື້ນ ທີ່ສະເພາະບາງພື້ນທີ່, ເປັນສາເຫດເຮັດໃຫ້ຄ້ອມພິວເຕີ ບໍ່ ສາມາດ ສະຕາດ ໄດ້ເລີຍ.
- ເພື່ອປ້ອງກັນສິ່ງນີ້, BIOS ແມ່ນມີ ຕົວເລືອກໃນການປ້ອງກັນການຂຽນ ໃສ່ boot sector ຂອງຊ່ອງສຽບໄດຣ ທາງນອກ

29/08/55

6

File ຫຼື Macro ໄວລັສ

- File ໄວລັສ ຕິດເຊື້ອຟາຍ ໜຶ່ງ ຫຼື ຫຼາຍຕົວໃນຄ້ອມພິວເຕີ.
- ແອັນຕີ ໄວລັສໃຊ້ bait files ເພື່ອຊອກເຫັນໄວລັສປະເພດນີ້. Bait files ມີຂະໜາດທີ່ຮູ້ໄດ້ ແລະ ມີໂຄງສ້າງທີ່ສາມາດກວດສອບໄດ້ກັບ ໂປຣແກ້ມ ແອັນຕີ ໄວລັສ.
- Macro ໄວລັສເປັນທີ່ພົບໄດ້ຫຼາຍໃນ ໂປຣແກຣມ Microsoft Office ປະເພດ ຟາຍ. ໃນລະບົບ ປະຕິບັດການ ວິນໂດສ ໂປຣແກຣມຕ່າງໆຂອງ ໄມໂຄຣຊອບແມ່ນມີຄຸນນະສົມບັດ ແລະ ໜ້າທີ່ຕ່າງທີ່ສາມາດສອຍໃຊ້ ໄດ້ງ່າຍ.
- Macro ໄວລສສາມາດປ້ອງກັນໂດຍ ການ ຕັ້ງຄ່າ disabling macros ໃຫ້ເປັນ default

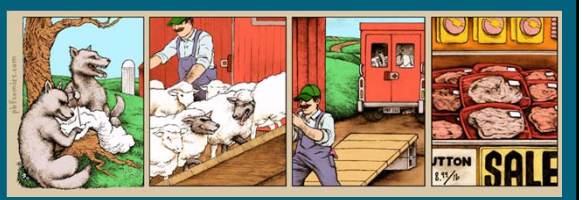
29/08/55 7

Polymorphic ໄວລັສ

- Polymorphic ໄວລັສຕິດເຊື້ອຕໍ່ຟາຍ ແລະ ມີການກ້ອບ ປີແບບ ເອັນຄິຣປ ດ້ວຍໂຕມັນເອງ, ເຊິ່ງ ສາມາດຕີໂຄດ ໂດຍການໃຊ້ ດີຄິຣປເຊິ່ນໂມດູ.
- ດີຄິຣປເຊິ່ນໂມດູ ແມ່ນມີການດັດແປງໄປເອງ ໃນການ ຕິດເຊື້ອແຕ່ລະຄັ້ງ
- ເຝັນໄວລັສ ທີ່ຂຽນຂຶ້ນມາໄດ້ດີ ເພາະວ່າບໍ່ມີສ່ວນທີ່ຄ້າຍຄື ກັນຫຼົງເຫຼືອຢູ່ໃນການ ຕິດເຊື້ອແຕ່ລະຄັ້ງ, ເຮັດໃຫ້ເປັນ ການຍາກໃນການຊອກເຫັນໂດຍກົງໂດຍການໃຊ້ signatures.

29/08/55 8

Joke..



29/08/55 9

ຄ້ອມພິວເຕີ Worm

- ຄ້ອມພິວເຕີ ເວີມ ແມ່ນເຟັ້ນ ມາວແວ ຄ້ອມພິວເ
  ໂປຣແກຣມທີ່ສາມາດສ້າງໂຕເອງຂຶ້ນໄດ້, ເຊິ່ງໃຊ້ລະບົບ
  ເຄືອຄ່າຍຄ້ອມພິວເຕີເພື່ອການສິ່ງ ກ໊ອບປີ ຂອງ**ມັນເອງ** ແຜ່
  ລາມອອກໄປດ້ວຍຕົວຂອງ**ມັນ**ເອງ
- ແຕກຕ່າງກັບ ໄວລັສ ຄ້ອມພິວເຕີຢູ່ບ່ອນວ່າ, ມັນບໍ່ຕ້ອງການທີ່ຈະຕິດ
  ພັນຕົວມັນເອງກັບໂປຣແກ້ມທີ່ມີຢູ່.
- **worms** ສ່ວນຫຼາຍແມ່ນຖືກສ້າງມາໃຫ້ແຜ່ເຊື້ອ ຫຼາຍກ່ວາການ
  ພະຍາຍາມ ຮຸກຮານ ຄ້ອມພິວເຕີທີ່ຜ່ານທາງ.
- ບາງຄັ້ງ ເຄື່ອງທີ່ຕິດເຊື້ອ ແມ່ນຕິດໂດຍ ຜູ້ທີ່ສິ່ງ spam ໃນຮູບຂອງ
  junk email

10

Trojan Horse

- **Trojan horse**, ຫຼື **Trojan**, ແມ່ນໂປຣແກຣມທີ່ທຳລາຍລະບົບນ້ຳທີ່
  ການເຮັດວຽກຂອງ ໂປຣແກຣມຕ່າງໆ.
- ຊອບແວ ເບິ່ງຄືວ່າເຮັດວຽກທຳມະດາທົ່ວໄປ ແຕ່ວ່າ ລັກເອົາຂໍ້ມູນ ແລະ
  ເປັນໄພຕໍ່ລະບົບຢູ່ເບື້ອງຫຼັງ.
- ແຕກຕ່າງກັບ viruses ຫຼື worms, Trojan horses ບໍ່ສາມາດ
  ກ໊ອບປີຕົວເອງໄດ້

Rootkit

- Rootkit ເປັນຊອບແວທີ່ເຊື່ອງຕົວເອງ **ແລະ**
  ເຮັດໃຫ້ຕົວເອງສາມາດເຂົ້າຄ້ອມພິວເຕີ້ໂດຍ
  ການລີ້ຊ້ອນຈາກ administrators
- Rootkit ແມ່ນຍາກໃນການກວດເຫັນ
  ເພາະວ່າ ມັນສາມາດເຊື່ອງຕົວເອງໃນ **ຊອບ**
  ແວທີ່ພະຍາຍາມຊອກຫາມັນ

29/08/55 12

ການປ້ອງກັນ

- ໃຊ້ຄວາມລະມັດລະວັງ
- ມີແອັນຕີໄວລັສທີ່ອັບເດດ
- ຕ້ອງເຮັດໃຫ້ຕິດ ສະແກ້ນໄວລັສ ອັບເດດຕະຫຼອດເວລາ
- ຕ້ອງໃຊ້ real-time file system protection ໃນແອັນຕີໄວລັສ
- ຄິດດີໆ ກ່ອນເປີດ e-mail attachments
- ຕ້ອງມີການ ແປ້ກອັບ ເອກະສານທີ່ສຳຄັນຕ່າງໆ ໃນອຸປະກອນທີ່ເປັນ read-only .
- ບໍ່ຄວນດາວໂລດ ສິ່ງທີ່ບໍ່ກ່ຽວກັບວຽກງານເຊັ່ນ: ໜັງ, ເກມສ ເປັນຕົ້ນ ໂດຍໃຊ້ ຄ້ອມພິວເຕີຂອງຫ້ອງການ.
- ຖ້າພາກ ສິ່ງໃສ ຫຼື ບໍ່ແນ່ໃຈວ່າແມ່ນໄວລັສ ຫຼື ບໍ່, ຕ້ອງຕິດຕໍ່ກັບ ພະນັກງານ ໄອທີ ໂດຍທັນທີ.

29/08/55

Virus scanner ໄວລັສສະແກ້ນເນ

- ໄວລັສ ສະແກນເນ ຕ້ອງໃຫ້ ອັບເດດ, ໂດຍ:
  - ເລືອກ ໄວລັສ ສະແກ້ນເນ ທີ່ ຟີຣ ແລະ ໃຊ້ງ່າຍ
  - ຕັ້ງ auto-update ເອງ
  - ຕັ້ງການ ສະແກນ ໝົດຄ້ອມພິວເຕີ ອາທິດລະຄັ້ງ
  - ຕັ້ງຄ່າ real-time scanning on ເພື່ອການປົກປ້ອງຄ້ອມພິວເຕີຕະຫຼອດ ການໃຊ້ງານ

14

ບົດສະຫຼຸບ

- ໄວລັສ ບໍ່ພຽງແຕ່ເປັນໄພເທົ່ານັ້ນ
- ເພື່ອທີ່ຈະຫຼີກລ້ຽງ ການຕິດເຊື້ອໄວລັສ ຈຳເປັນຕ້ອງ:
  - ຕັ້ງໄວລັສ ສະແກ້ນເນ ໃຫ້ ອັບເດດ
  - ຫ້າມດາວໂລດ ໂປຣແກມ ຫຼື ເກມຕ່າງໆໂດຍໃຊ້ຄ້ອມພິວເຕີຫ້ອງການ
  - ລະວັງການ ສຽບ ແລະ ໃຊ້ USB - ສະແກ້ນກ່ອນ!!!!
  - Disable ການຂຽນ boot-sector ຈາກ BIOS
  - ລະວັງ spam mail ແລະ links ທີ່ສົງໃສຕ່າງໆກັບ ອີເມວ ຫຼື ເວບໄຊ.

29/08/55

16


ຂອບໃຈ
ຫຼາຍໆ