Malware propagation through software piracy

Jacomo Piccolini
Introduction:

- Software piracy is being used as a vector to propagate malicious code
- Software piracy has many faces
- Infected machines generates profit to miscreants…
Information collected:

- Popular software were searched for cracks, serial numbers, keygens (serial number generators) and unauthorized distributions.
- Search using P2P networks, IRC and simple web surfing.
- 4,405 files of cracks, keygens and serials were collected in total of +3.8gigs of files
Malware propagation through software piracy

Information collected:

- 322 related to Windows XP WGA
- 17 related to IE7 and WMP11
- 172 related to Windows Vista Activation
- 61 related to DVD burning
- 85 related to antivirus software
- 6 related to anti-spyware
Malware propagation through software piracy

Information collected: (after unpacking)

- 2115 .exe files
- 1634 .zip files
- 1279 .rar files
- 2075 .txt files
- 585 .dll files

- 97 password-protected files (need to register or pay to unpack)
Information collected (common names):

“Generate Genuine Serial For WinXP.exe”
“Change WinXP Key.exe”
“WinXP Genuine Advantage Fix.exe”
“WGAFixer v3.3 (1.5.540.0)-Taag.exe”
“WGA Notification Removal.exe”
“Install_MSN_Messenger_DL.exe”
“Windows XP SP2 Keygen + Key Changer + WGA Validation.rar”
“Windows Xp Wga Windows Genuine Advantage Validation Crack 1.5.532.0 Legitcheckcontrol Dll Wgalogon Dll Wgatray Exe.zip”
“WGA Patcher Permanent Kit-1-1-2007.rar”
“Wga Microsoft Windows Genuine Advantage Crack Fix Full 1Click 2007.zip”
Malware propagation through software piracy

Search responses:

- You can search for the craziest crack and serial and you will find it: try search for “this is a malware test response”
The Spongebob effect:

• Why not? spongebob operating system 4.8 crack serial

We should consider that malicious code can be built on demand based on user activity or search query
Piracy:

- Why do people go for software piracy?
  - **Price?** How many Big Macs you need to buy a Windows Vista Business?
  - Brazil $BM 123 for a Vista
  - EUA $BM 93 for a Vista
  - Germany $BM 53 for a Vista (thanks Peter Quick)
  - China $BM 157 for a Vista (thanks CERT/CN)
  - Malaysia $BM 176 for a Vista (thanks MyCERT)

- The latest ultimate version?
  - Consumers are getting crazy for new versions and products. People are hacking into development companies to steal delayed products (Condition Zero, game).
    They also download fake servicepack files just because their version is newer (servicepack 3 for Windows XP).
Malware propagation through software piracy

Source of evil:

- P2P networks
- Search engines
- IRC cracking channels
- Street CDs
- Friends
Source of evil:

• Search engines are fighting this issue

Warning - visiting this web site may harm your computer!

You can learn more about harmful web content and how to protect your computer at StopBadware.org.

Suggestions:

• Return to the previous page and pick another result.
• Try another search to find what you're looking for.

Or you can continue to http://crackspider.net/need/crack/windowsmediaplayer11.html at your own risk.

Advisory provided by Google

Brazilian Research and Academic Network CSIRT
Malware information:

- From the 4.405 files collected, 2.858 were executables. The 4.405 files generated 47,530 files after recursive unpacking.

- From the 2.858 executables, 1.801 were classified as malicious: 63%
  Infection rate from all downloaded files: 40%
Malware information:

- 65% of malware collected was classified as downloaders (additional malicious code will be downloaded upon execution)
- 35% of malware collected were bot infection files
- 20% of all files have any kind of spyware/adware functionalities (browser hijacking, etc)
Malware information: antivirus results

- 46 types of malware
  - Adware.Advertmen-1
  - AdWare.BHO-2
  - Adware.Casino
  - Dialer-182
  - Trojan.Clicker
  - Trojan.Downloader
  - Trojan.Dragonbot
  - Trojan.Dropper
  - Trojan.Keylogger
  - Trojan.Packed
  - Trojan.Proxy
  - Trojan.Spambot
  - Worm.Bagle
  - Worm.Drefir
  - Worm.P2P.KWBot
  - Worm.Puce

---

This is very bad

This is bad

This is very bad

This is bad

This is bad

All this make money to miscreants
Malware propagation through software piracy

Malware packer information:

• 61 types of packers (from .exe files)
  – 39% UPX all versions
  – 13% Winrar
  – 11% FSG
  – 10% PE_COMPACT
  – 5% ASPack

Infection rate over 1801 executables: 63%
Infection rate over PE_COMPACT and ASPack: 95%
Malware propagation through software piracy

• Worst case scenario:
  – People with pirated operating system and no patches (they need to validate) looking for a pirate version of a commercial antivirus to use in order to be protected!
  – High percentage of files related to software piracy are malicious (there is no safe ground).
  – Antivirus efficiency needs to be improved.
  – Packers should be banned?
Malware propagation through software piracy

• Questions?

• Contact: jacomo@cais.rnp.br