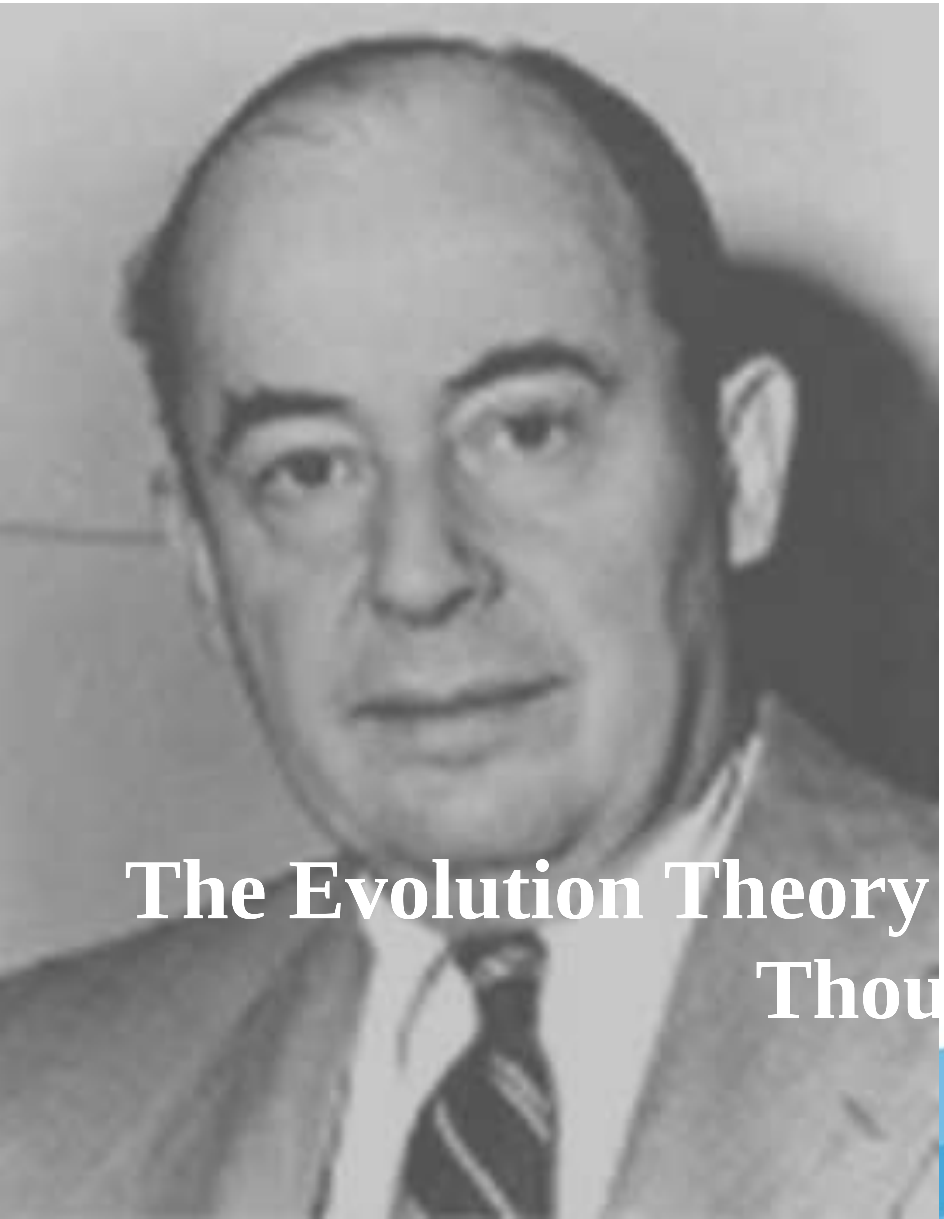
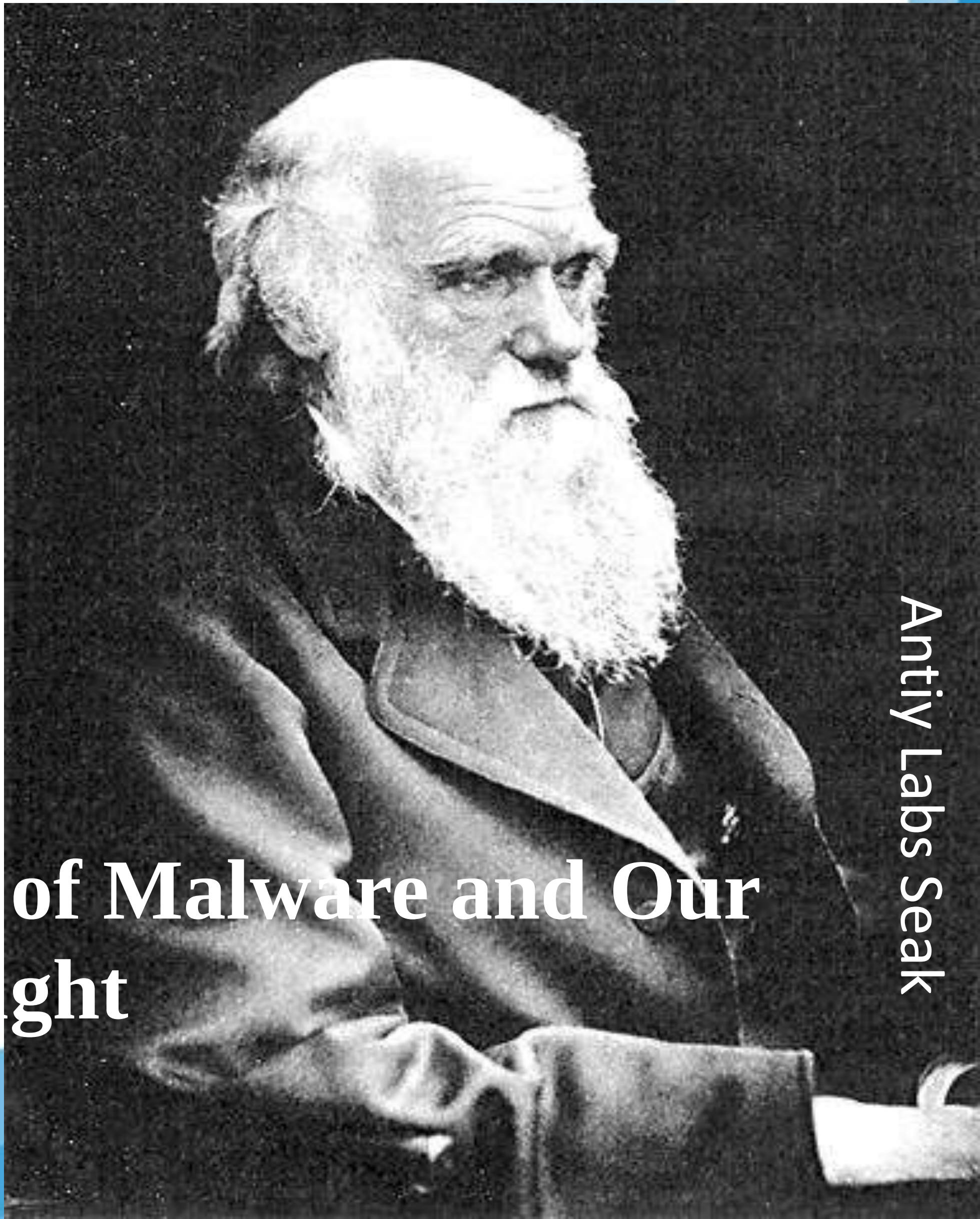




The Evolution Theory of Malware and Our Thought

Antiy Labs Seak

Warn

The views as well as the visual effects of pictures in the report may cause some displeasures, so it is not suitable to watch after meals.

Outline

- The evolution of Antivirus
- The virus ecology in the Evolution Theory
- Lamarck，Darwin，and AI Empire
- I am the nature—thinking on the creating and struggling
- Meditating in front of Darwin’ s portrait

The evolutionary methods of AV

Fighting against directly	• Anti-virus
Adding functions	• Regmon and TDI mon
Induction to normalization	• From AntiOOB to PFW
Reflux	• Immunity
Conversion between foreground and background	• Unknown detection based on neural network and Decision Tree
Introduction	• UTM added AV Engine
Hardware and software	• Anti-virus card -〉 anti-virus software
……	

Outline

- The conclusive history of AV vs. VX
- The virus ecology in the Evolution Theory
- Lamarck, Darwin, and AI Empire
- I am the nature—thinking on the creating and struggling
- Meditating in front of Darwin’s portrait

Darwin, as a naturalist, sailed with HMS *Beagle* for 5 years.

The picture is about the anchorage of HMS *Beagle* on July, 5th, 1832.

Form Stowe, K. (1995) "Exploring Ocean Science", 2th ed.

The Evolution Theory of Malware: the Chapter of Living

- The status of Malware, similar to that of the living creatures， is the result of the comprehensive elimination and selection． Actually， it is the same with all the software programs．

- The living creatures developed the survival ability during the long-term antagonism， elimination and selection．

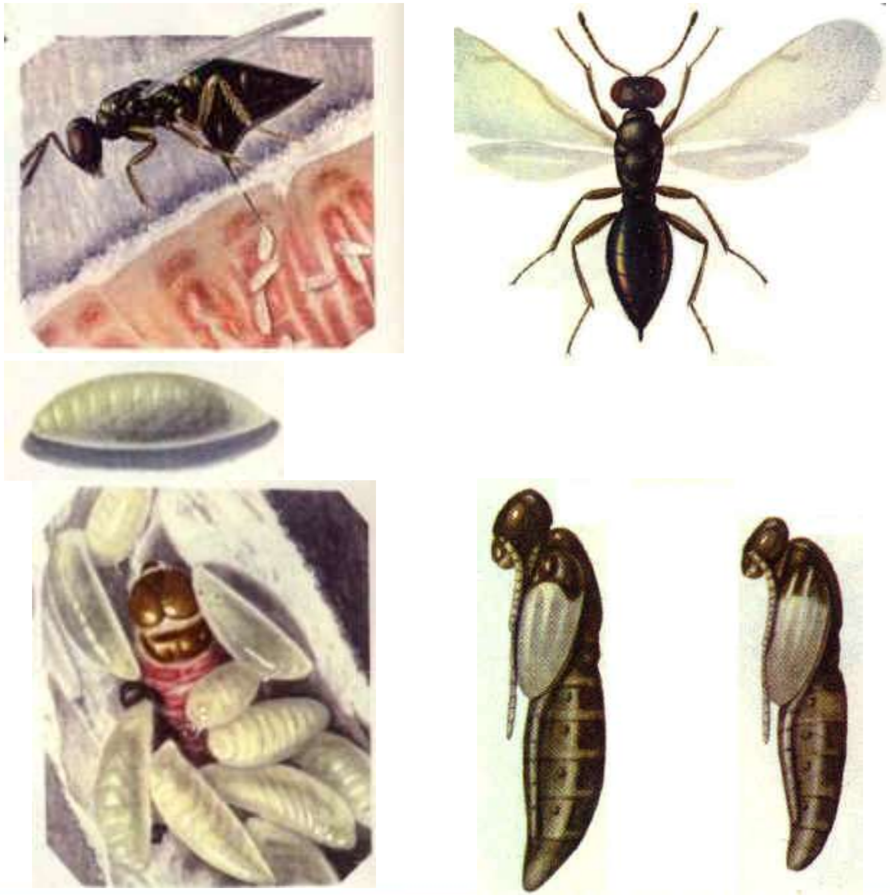
- Let’s come to the Chapter of Living

Parasitism

The infection of files and boot sectors

- The most primitive skills of viruses
- Keeping the infected objects the same as original ones until the viruses begin to attack

Nasonia



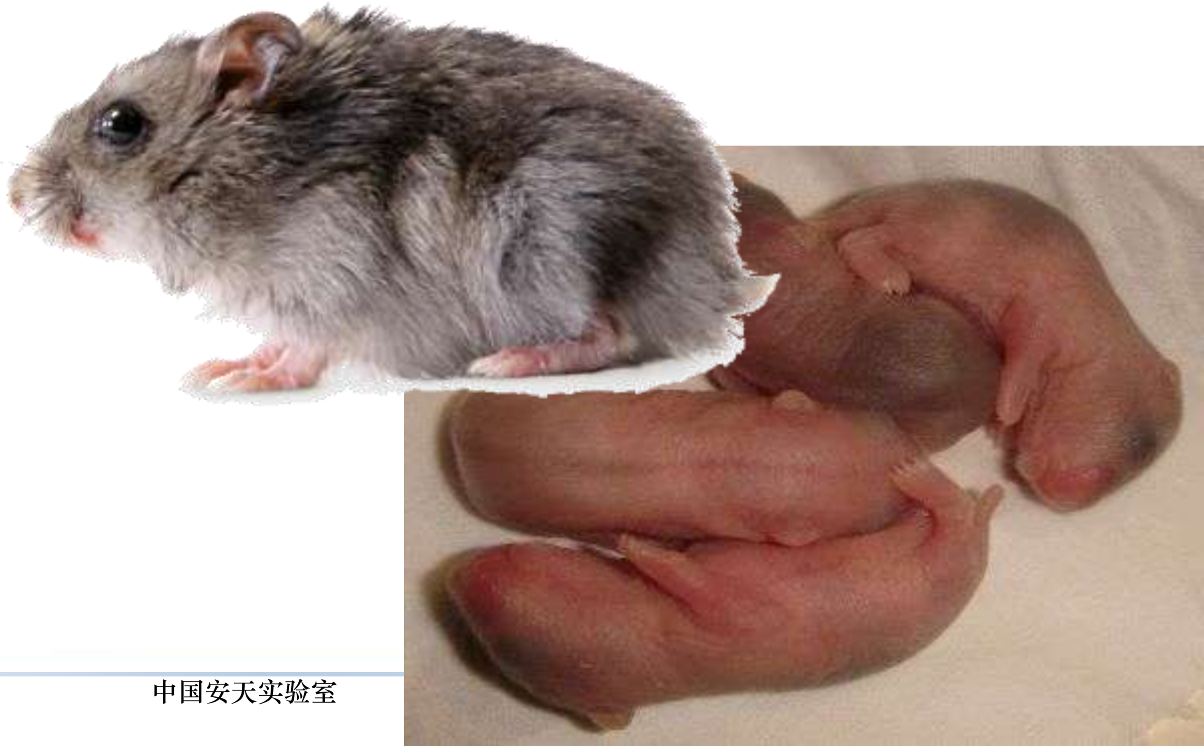
Reproduction

Self-replicating

- SQL.Slammer worm has infected seventy-five thousand(75,000) computers in just ten minutes across the world.

Self-reproducing with a large number

- There is an old saying that a male mouse and a female mouse can breed two hundred and fifty babies in three years.



Avoiding Predators

Yankee

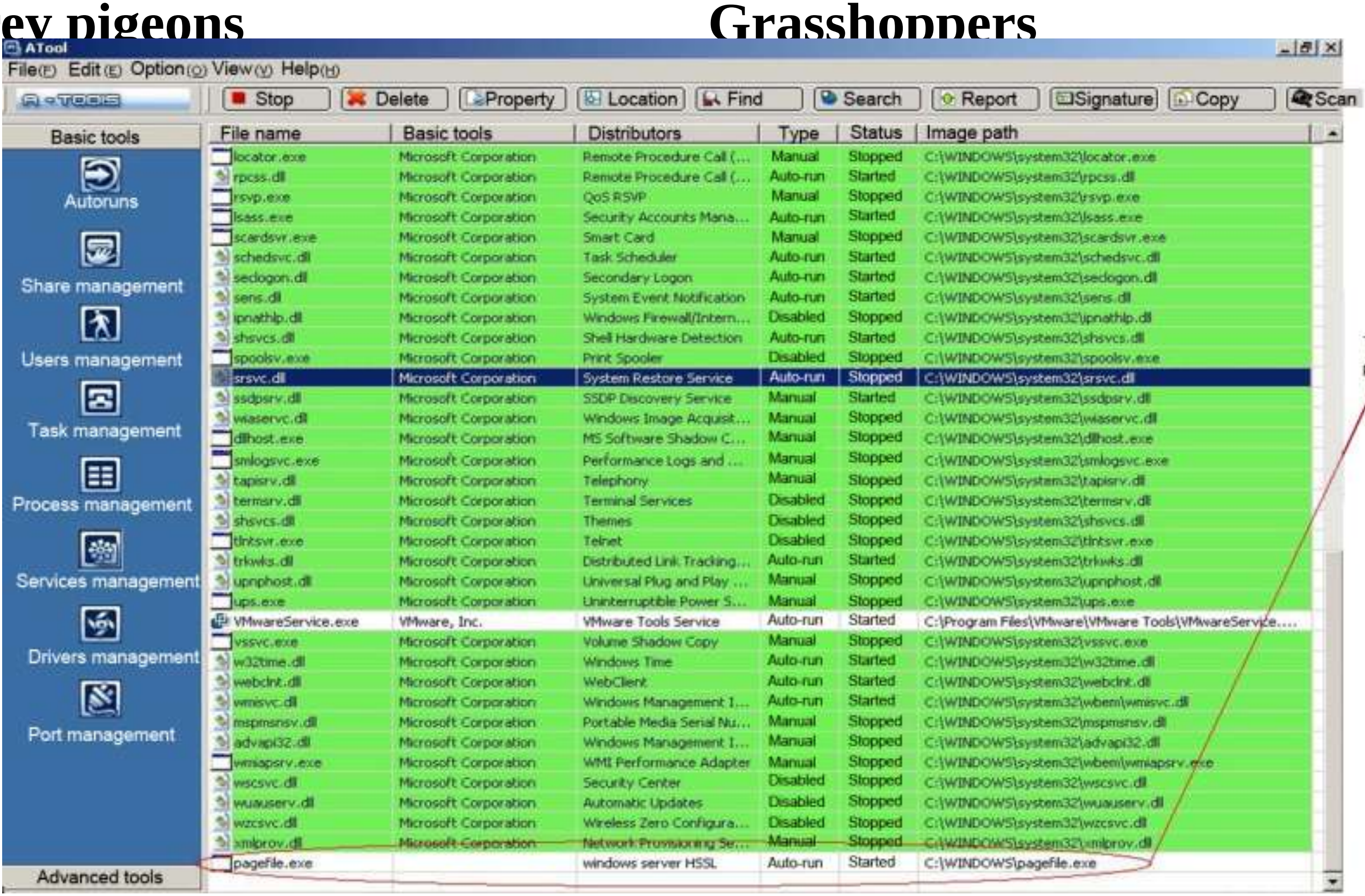
- Yankee was found by displaying the songs of Yankee Doodle and became well-known.
- Yankee is one of the earliest viruses which can avoid their predators. It will “run away” when finding the Debug module.

Meerkat

Protective Coloration

Grey pigeons

Grasshoppers

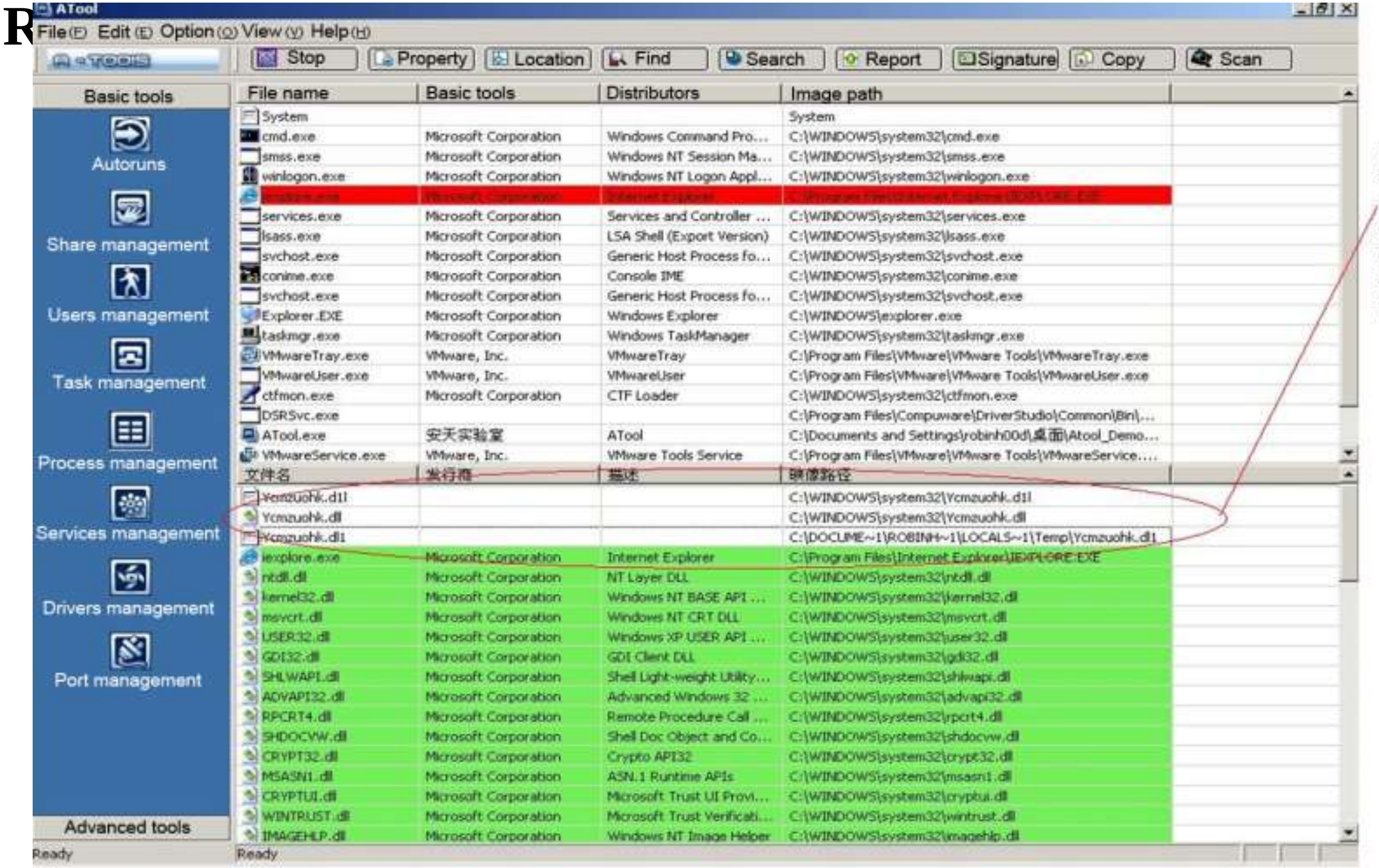


File name	Basic tools	Distributors	Type	Status	Image path
locator.exe	Microsoft Corporation	Remote Procedure Call (…	Manual	Stopped	C:\WINDOWS\system32\locator.exe
rpcss.dll	Microsoft Corporation	Remote Procedure Call (…	Auto-run	Started	C:\WINDOWS\system32\rpcss.dll
rsvp.exe	Microsoft Corporation	QoS RSVP	Manual	Stopped	C:\WINDOWS\system32\rsvp.exe
lsass.exe	Microsoft Corporation	Security Accounts Mana…	Auto-run	Started	C:\WINDOWS\system32\lsass.exe
scardsvr.exe	Microsoft Corporation	Smart Card	Manual	Stopped	C:\WINDOWS\system32\scardsvr.exe
schedsvc.dll	Microsoft Corporation	Task Scheduler	Auto-run	Started	C:\WINDOWS\system32\schedsvc.dll
seclogon.dll	Microsoft Corporation	Secondary Logon	Auto-run	Started	C:\WINDOWS\system32\seclogon.dll
sens.dll	Microsoft Corporation	System Event Notification	Auto-run	Started	C:\WINDOWS\system32\sens.dll
ipnathlp.dll	Microsoft Corporation	Windows Firewall/Intern…	Disabled	Stopped	C:\WINDOWS\system32\ipnathlp.dll
shsvcs.dll	Microsoft Corporation	Shell Hardware Detection	Auto-run	Started	C:\WINDOWS\system32\shsvcs.dll
spoolsv.exe	Microsoft Corporation	Print Spooler	Disabled	Stopped	C:\WINDOWS\system32\spoolsv.exe
srsvc.dll	Microsoft Corporation	System Restore Service	Auto-run	Stopped	C:\WINDOWS\system32\srsvc.dll
ssdpsrv.dll	Microsoft Corporation	SSDP Discovery Service	Manual	Started	C:\WINDOWS\system32\ssdpsrv.dll
wiaservc.dll	Microsoft Corporation	Windows Image Acquisit…	Manual	Stopped	C:\WINDOWS\system32\wiaservc.dll
dllhost.exe	Microsoft Corporation	MS Software Shadow C…	Manual	Stopped	C:\WINDOWS\system32\dllhost.exe
smlogsvc.exe	Microsoft Corporation	Performance Logs and …	Manual	Stopped	C:\WINDOWS\system32\smlogsvc.exe
tapisrv.dll	Microsoft Corporation	Telephony	Manual	Stopped	C:\WINDOWS\system32\tapisrv.dll
termsrv.dll	Microsoft Corporation	Terminal Services	Disabled	Stopped	C:\WINDOWS\system32\termsrv.dll
shsvcs.dll	Microsoft Corporation	Themes	Disabled	Stopped	C:\WINDOWS\system32\shsvcs.dll
tlntsvr.exe	Microsoft Corporation	Telnet	Disabled	Stopped	C:\WINDOWS\system32\tlntsvr.exe
trkwks.dll	Microsoft Corporation	Distributed Link Tracking…	Auto-run	Started	C:\WINDOWS\system32\trkwks.dll
upnphost.dll	Microsoft Corporation	Universal Plug and Play …	Manual	Stopped	C:\WINDOWS\system32\upnphost.dll
ups.exe	Microsoft Corporation	Uninterruptible Power S…	Manual	Stopped	C:\WINDOWS\system32\ups.exe
VMwareService.exe	VMware, Inc.	VMware Tools Service	Auto-run	Started	C:\Program Files\VMware\VMware Tools\VMwareService.…
vssvc.exe	Microsoft Corporation	Volume Shadow Copy	Manual	Stopped	C:\WINDOWS\system32\vssvc.exe
w32time.dll	Microsoft Corporation	Windows Time	Auto-run	Started	C:\WINDOWS\system32\w32time.dll
webclnt.dll	Microsoft Corporation	WebClient	Auto-run	Started	C:\WINDOWS\system32\webclnt.dll
wmisvc.dll	Microsoft Corporation	Windows Management I…	Auto-run	Started	C:\WINDOWS\system32\wbem\wmisvc.dll
mspmsnsv.dll	Microsoft Corporation	Portable Media Serial Nu…	Manual	Stopped	C:\WINDOWS\system32\mspmsnsv.dll
advapi32.dll	Microsoft Corporation	Windows Management I…	Manual	Stopped	C:\WINDOWS\system32\advapi32.dll
wmiapsrv.exe	Microsoft Corporation	WMI Performance Adapter	Manual	Stopped	C:\WINDOWS\system32\wbem\wmiapsrv.exe
wscsvc.dll	Microsoft Corporation	Security Center	Disabled	Stopped	C:\WINDOWS\system32\wscsvc.dll
wuauserv.dll	Microsoft Corporation	Automatic Updates	Disabled	Stopped	C:\WINDOWS\system32\wuauserv.dll
wzcsvc.dll	Microsoft Corporation	Wireless Zero Configura…	Disabled	Stopped	C:\WINDOWS\system32\wzcsvc.dll
xmlprov.dll	Microsoft Corporation	Network Provisioning Se…	Manual	Stopped	C:\WINDOWS\system32\xmlprov.dll
pagefile.exe		windows server HSSL	Auto-run	Started	C:\WINDOWS\pagefile.exe

The services created
pigeon for auto-start

Mimicry

R



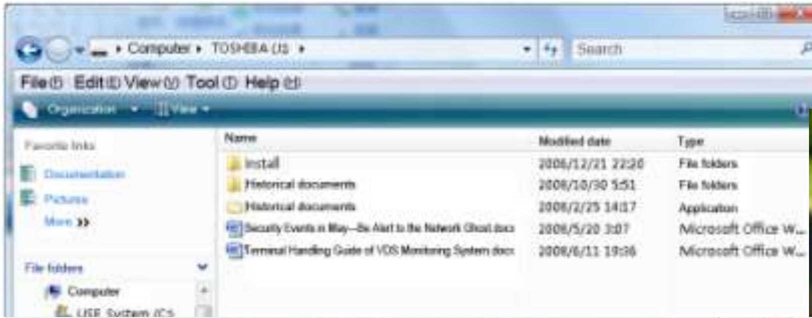
File name	Basic tools	Distributors	Image path
System			System
cmd.exe	Microsoft Corporation	Windows Command Pro...	C:\WINDOWS\system32\cmd.exe
smss.exe	Microsoft Corporation	Windows NT Session Ma...	C:\WINDOWS\system32\smss.exe
winlogon.exe	Microsoft Corporation	Windows NT Logon Appl...	C:\WINDOWS\system32\winlogon.exe
iexplore.exe	Microsoft Corporation	Internet Explorer	C:\Program Files\Internet Explorer\IEXPLORE.EXE
services.exe	Microsoft Corporation	Services and Controller ...	C:\WINDOWS\system32\services.exe
lsass.exe	Microsoft Corporation	LSA Shell (Export Version)	C:\WINDOWS\system32\lsass.exe
svchost.exe	Microsoft Corporation	Generic Host Process fo...	C:\WINDOWS\system32\svchost.exe
conime.exe	Microsoft Corporation	Console IME	C:\WINDOWS\system32\conime.exe
svchost.exe	Microsoft Corporation	Generic Host Process fo...	C:\WINDOWS\system32\svchost.exe
Explorer.EXE	Microsoft Corporation	Windows Explorer	C:\WINDOWS\explorer.exe
taskmgr.exe	Microsoft Corporation	Windows TaskManager	C:\WINDOWS\system32\taskmgr.exe
VMwareTray.exe	VMware, Inc.	VMwareTray	C:\Program Files\VMware\VMware Tools\VMwareTray.exe
VMwareUser.exe	VMware, Inc.	VMwareUser	C:\Program Files\VMware\VMware Tools\VMwareUser.exe
ctfmon.exe	Microsoft Corporation	CTF Loader	C:\WINDOWS\system32\ctfmon.exe
DSRSvc.exe			C:\Program Files\Compuware\DriverStudio\Common\Bin\...
ATool.exe	安天实验室	ATool	C:\Documents and Settings\robinh00d\桌面\Atool_Demo...
VMwareService.exe	VMware, Inc.	VMware Tools Service	C:\Program Files\VMware\VMware Tools\VMwareService....

文件名	发行商	描述	映像路径
Ycmzuohk.d1l			C:\WINDOWS\system32\Ycmzuohk.d1l
Ycmzuohk.dll			C:\WINDOWS\system32\Ycmzuohk.dll
Ycmzuohk.dl1			C:\DOCUME~1\ROBINH~1\LOCALS~1\Temp\Ycmzuohk.dl1
iexplore.exe	Microsoft Corporation	Internet Explorer	C:\Program Files\Internet Explorer\IEXPLORE.EXE
ntdll.dll	Microsoft Corporation	NT Layer DLL	C:\WINDOWS\system32\ntdll.dll
kernel32.dll	Microsoft Corporation	Windows NT BASE API ...	C:\WINDOWS\system32\kernel32.dll
msvcrt.dll	Microsoft Corporation	Windows NT CRT DLL	C:\WINDOWS\system32\msvcrt.dll
USER32.dll	Microsoft Corporation	Windows XP USER API ...	C:\WINDOWS\system32\user32.dll
GDI32.dll	Microsoft Corporation	GDI Client DLL	C:\WINDOWS\system32\gdi32.dll
SHLWAPI.dll	Microsoft Corporation	Shell Light-weight Utility...	C:\WINDOWS\system32\shlwapi.dll
ADVAPI32.dll	Microsoft Corporation	Advanced Windows 32 ...	C:\WINDOWS\system32\advapi32.dll
RPCRT4.dll	Microsoft Corporation	Remote Procedure Call ...	C:\WINDOWS\system32\rpcrt4.dll
SHDOCVW.dll	Microsoft Corporation	Shell Doc Object and Co...	C:\WINDOWS\system32\shdocvw.dll
CRYPT32.dll	Microsoft Corporation	Crypto API32	C:\WINDOWS\system32\crypt32.dll
MSASN1.dll	Microsoft Corporation	ASN.1 Runtime APIs	C:\WINDOWS\system32\msasn1.dll
CRYPTUI.dll	Microsoft Corporation	Microsoft Trust UI Provi...	C:\WINDOWS\system32\cryptui.dll
WINTRUST.dll	Microsoft Corporation	Microsoft Trust Verificati...	C:\WINDOWS\system32\wintrust.dll
IMAGEHLP.dll	Microsoft Corporation	Windows NT Image Helper	C:\WINDOWS\system32\imagehlp.dll

The sub-modules hiding the process iexplorer.exe are checked with signature, and three of them are found to be unsigned.

Allure

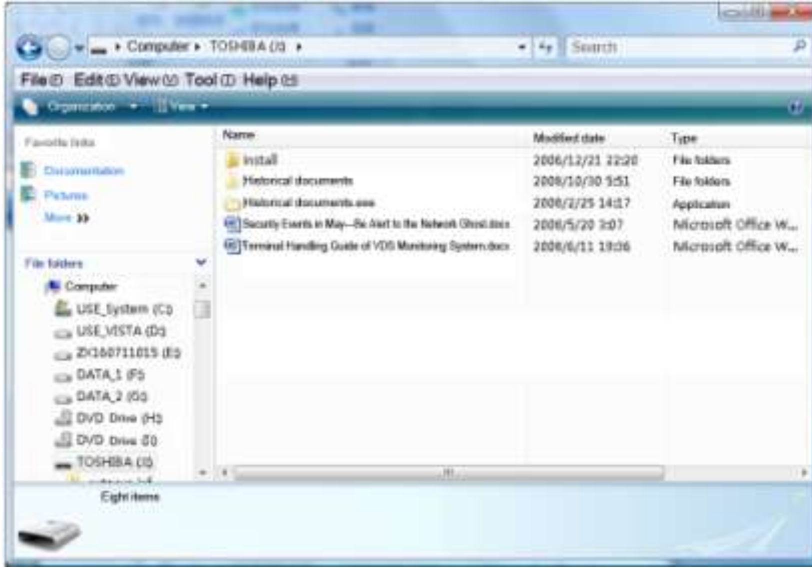
Social engineering means



Computer ▸ TOSHIBA (J:) ▸

File(F) Edit(E) View(V) Tool(T) Help(H)

Name	Modified date	Type
Install	2006/12/21 22:20	File folders
Historical documents	2008/10/30 5:51	File folders
Historical documents	2008/2/25 14:17	Application
Security Events in May—Be Alert to the Network Ghost.docx	2008/5/20 3:07	Microsoft Office W...
Terminal Handling Guide of VDS Monitoring System.docx	2008/6/11 19:36	Microsoft Office W...



Computer ▸ TOSHIBA (J:) ▸

File(F) Edit(E) View(V) Tool(T) Help(H)

Name	Modified date	Type
Install	2006/12/21 22:20	File folders
Historical documents	2008/10/30 5:51	File folders
Historical documents.exe	2008/2/25 14:17	Application
Security Events in May—Be Alert to the Network Ghost.docx	2008/5/20 3:07	Microsoft Office W...
Terminal Handling Guide of VDS Monitoring System.docx	2008/6/11 19:36	Microsoft Office W...

Eight items

The snail a kind of fluke hosts on

Suspended Animation

Rootkit.Baidu

- To intercept the API operation of anti-virus software. When finding the Deletefile, it shows SUCCESS.

- The anti-virus software can detect files circularly, so it changes the interception policy.

A millipede in suspended animation

The Evolution Theory of Malware: the Chapter of Death

- Trilobites, dinosaurs, saber-toothed tiger have died out, and the South China tigers are about to die out.
- The dead ones left fossils and the dying ones are surviving in the zoos.
- The thinking tank of Pakistan and the Morris worm are no longer active. Some of Malwares are at the edge of the attacking field.
- The viruses, with no activities, are not harmful any more, and just the source codes or disassembly codes printed in textbooks.

Predators

Security Points

- Anti-virus
- Defense

Living Cretures

- Preying
- Enhancing immunity to avoid being hosted on

Environment

- A variety of viruses have been eliminated due to the upgrading of the operation systems.
- DOS 3.3 >DOS 5
- MZ > PE
- Ring0
- VxD->WDM

Propagation and Migration

- The exchanging methods of main data to Malware are as important as the migrating ways to animals.
- Disks
- E-mails
- Remote exploits
- Password cracking
- USB Flash Drive
- WEB injection

VX: not the only one to be eliminated

- OLE2 Watershed
- The security mechanisms like DEP and PatchGuard enhanced by Vista, stop the viruses outside the computers but interrupt the anti-virus vendors’ incapability test for a long time.

The Evolution Theory of Malware:
the Chapter of Mutation

The core of the evolution is to architect the academic system with the hard evidence of the Origin of Species and Evolution rather than breeding and life-death. This kind of academic system can overthrow the fallacy that God created the world and the species remained unchanged.

Variants of the Virus Family

- That the Jerusalem had three hundred and fifty-four variants in DOS time seemed to be unbelievable.

- At present, there are thousands of variants of virus families which do not include the variants matched out by general features.

- The number of the grey pigeon variants accounts for 17percent of the total backdoor variants in the world.

A Typical Case to Revisit the Anti-immunity

- The modification and evolution of the propagation.

Disassembly and Code Evolution

- The wide propagation of DOS virus attributes to the disclosure of disassembly results.
- The crazy increasing of backdoors disclosed on BO.
- The appearance of Rbot with most variants owing to the code disclosure.

The Binary Evolution

- The evolution of password guessing worms

Worm.ronron.a -> Worm.ronron.b

└Cloner ->STED -> eleet

cals->olo

Release

Worm.Dvldr

Cross-platform Virus: not the Product of Variation

- Do the double-state viruses PE and ELF belong to variation?
- Do the double-state viruses Macro and DOS.com

  belong to variation?
- Regarding them as amphibians

The Change of State Does Not Mean Self-variation

- No new features will not be invented in the process of virus variation. we can call it chameleon.
- We can call it chameleon.

The Evolution Theory of Malware:
the Chapter of Anecdotes

- Interesting Phenomenon

Wildlist VS Zoo

Wildlist

Zoo

The Secret of Longevity

- Klez
- Parite
- wyx

Species in the Legend

Overwhelming Rumors

- The e-mail virus
- The IM information virus
- The BIOS virus

Manufacturing Species

Outline

- The conclusive history of AV vs. VX
- The virus ecology in the Evolution Theory
- Lamarck, Darwin, and AI Empire
- I am the nature—thinking on the creating and struggling
- Meditating in front of Darwin’s portrait

Darwin or Lamarck?

Lamarckism

- Evolution is the result of biological activity.
  - Use and disuse
  - Inheritance of acquired characteristics

Darwinism

- Evolution is the result of natural selection.
  - Inheritance with uncertainty
  - The uncertainty eliminated by environment

Electing Darwin

- The malware has no tendency to evolve by itself.
- The result of natural selection is that some malwares

  dying out and some malwares being active.

The Confusion

- If we consider virus and anti-virus software as animals, the people who work on them belong to environment or are the “creator”?

- Both VX and AV mutate owing to the experience and attempt of human beings.

- Living creatures breed and are bred in the process of mutating; codes copy and are copied in constance.

- The creators and the modificators are the parts of the inherited strand, which are the biggest difference from the Code Darwinism.

Is it possible for malware to evolve in a Lamarckian way?

- The uncertainty of malware evolution is the transformation of biological activity.
- Is it possible for malware to evolve in a Lamarckian way?

The Ideal Achievements of Self-study

- Picking up the unknown viruses with Neural Networks

Distributed Nightmares

- Based on powerful computing ability.

- The computing ability of AI built with single point

  will not reach the level of children after ten years.

- How is about the bot of hundreds of thousands of

  computers?

Outline

- The conclusive history of AV vs. VX
- The virus ecology in the Evolution Theory
- Lamarck, Darwin, and AI Empire
- I am the nature—thinking on the creating and struggling
- Meditating in front of Darwin’s portrait

Why the red pines began to release such large amounts of carbon dioxide?

The pine beetles have destroyed 12.8 square kilometers of forest in western Canada by the end of 2006. It is not the first time for the forest destroyed at this level, but the destruction is 10 times as serious as before.

The beetles will release large amounts of carbon dioxide after the trees die?

Protecting the Trees or Killing the Beetles?

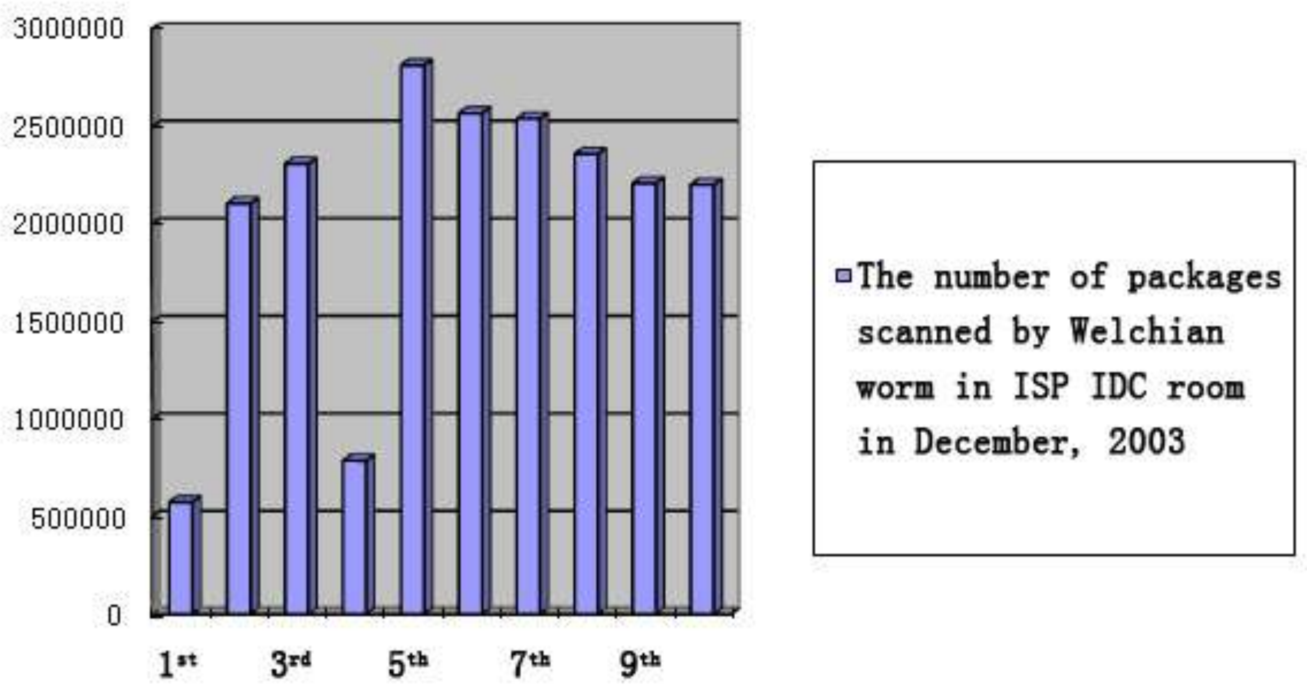
- The purpose of AVER is to maintain the system running normally.
- Recalling the key points in the “war”
- welchian
- Sobig.f
- Dvlodr
- downloader
- MS08-067

Dvloder

- Dvloder is the most dangerous one of password guessing worms.
- Larger password files, faster scanning speeds.
- More compact ways to combine together.
- Setting up VNC backdoor.
- HIT-Antiy CERT (built by HIT and Antiy) found it first, and located the earliest infected computer very fast.

Welchian

- The adoption of ARP repression and the manipulation of unmanagable network



The monitoring result of a HIT mail server someday

Rank	Name	Times	Traffic
1	I-Worm.sobig	39006	3.7G
2	I-worm.klez.h	34664	5.6G
3	I-Worm.Runonce	34206	3.0G
Amount			12.3G

The Process of Downloader

- The identification of behaviors

- DEMO

The Response to MS08-067

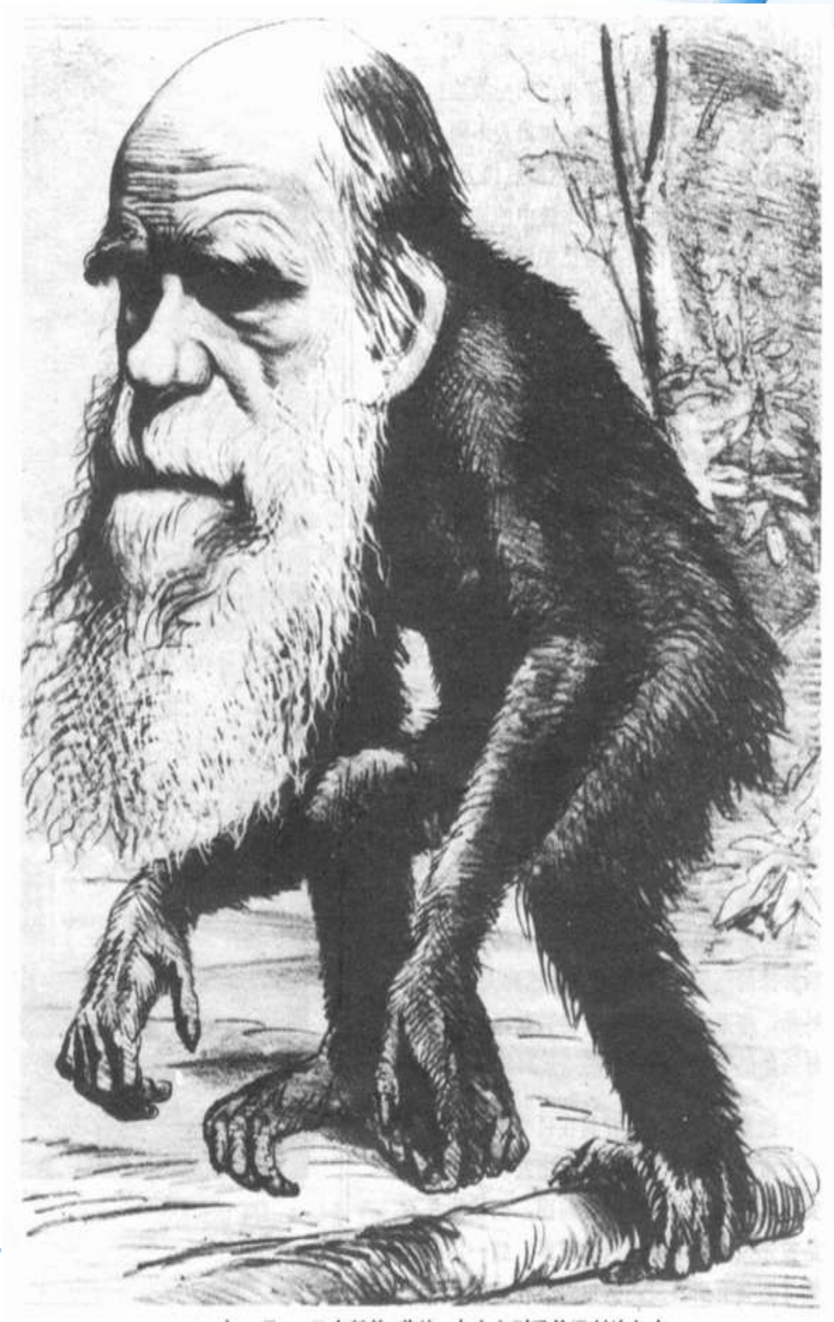
- Min loading and scanning probe

- Class C, 11 severs

Outline

- The conclusive history of AV vs. VX
- The virus ecology in the Evolution Theory
- Lamarck, Darwin, and AI Empire
- I am the nature—thinking on the creating and struggling
- Meditating in front of Darwin’s portrait

Religious fanatics ridicule Darwin because he believes apes are our ancestors. Actually, Darwin just says human beings and apes have the same ancestors rather than to say that.



On AVER’s Defense

- AVER=Extortioner？
- AVER has determined the attributes of thousands of documents, analyzed millions of virus samples, extracted more than one million detection rules and named over 340 thousand viruses in past 20 years.
- Snort takes respected place in academia with less than 3 thousand (3,000) rules so far.

Thank you!

- Seak
- http://www.anity.com
- seak@antiy.net