

安天实验室
江海客

恶意代码的进化论 与我们的思考

警告

- 本报告中的观点以及图片的视觉效果可能引起人的不快，不适宜饭后观看。

提纲

- Antivirus的演进
- 进化论弦窗中的病毒生态
- 拉马克、达尔文和AI帝国
- 我即自然——造物与斗争的思考
- 在达尔文像前沉思

AV基本演进方法

直接对抗

- 专杀

功能增加

- Regmon/TDI mon

归纳-归一化

- 从AntiOOB到PFW

回流

- 免疫

前后台转化

- 基于神经网络/决策树未知检测

引入

- UTM增加AV Engine

硬件（设备）化/软件化

- 防毒卡-〉反病毒软件

.....

提纲

- 被定论的AV、VX对抗史
- 进化论弦窗中的病毒生态
- 拉马克、达尔文和AI帝国
- 我即自然——造物与斗争的思考
- 在达尔文像前沉思

达尔文以博物学家身份随着著小猎犬号 (HMS *Beagle*) 航行了五年，
图为小猎犬号於1832年7月5日泊於Rio de Janeiro外海的情形。
摘自Stowe, K.



恶意代码进化论.生篇

- 与生物形态一样，恶意代码的当前形态，是综合的淘汰和选择推动的结果。实施上这个情况适用于所有的软件程序。
- 在长期的对抗、淘汰和选择中生物具备了求生的本能。
- 请看生篇.....

寄生

文件、引导区感染

- 病毒的最原始技能
- 感染后保持对象原装，直到病毒发作

金小蜂



繁殖

自我复制

- SQL.Slammer蠕虫在十分钟之内感染了7.5万台计算机，

大量的自我繁殖

- 一公一母，三年二百五



躲避天敌

Yankee 📢

- 一个古老的病毒，发作现象是演奏乐曲，<Yangkee DooDle>
- Yankee具有最早的躲避天敌的能力的病毒之一，当其发现Debug加载时，便逃之夭夭。

狐獴



保护色

ATool

文件(F) 编辑(E) 选项(O) 查看(V) 帮助(H)

停止 删除 属性 定位 查找 搜索 上报 签名 复制

基本工具	文件名	发行商	描述	类型	状态	映像路径
	locator.exe	Microsoft Corporation	Remote Procedure Call (...	手动	已停止	C:\WINDOWS\system32\locator.exe
	rpcss.dll	Microsoft Corporation	Remote Procedure Call (...	自动	已启动	C:\WINDOWS\system32\rpcss.dll
	rsvp.exe	Microsoft Corporation	QoS RSVP	手动	已停止	C:\WINDOWS\system32\rsvp.exe
	lsass.exe	Microsoft Corporation	Security Accounts Mana...	自动	已启动	C:\WINDOWS\system32\lsass.exe
	scardsvr.exe	Microsoft Corporation	Smart Card	手动	已停止	C:\WINDOWS\system32\scardsvr.exe
	schedsvc.dll	Microsoft Corporation	Task Scheduler	自动	已启动	C:\WINDOWS\system32\schedsvc.dll
	seclogon.dll	Microsoft Corporation	Secondary Logon	自动	已启动	C:\WINDOWS\system32\seclogon.dll
	sens.dll	Microsoft Corporation	System Event Notification	自动	已启动	C:\WINDOWS\system32\sens.dll
	ipnathlp.dll	Microsoft Corporation	Windows Firewall/Intern...	禁止	已停止	C:\WINDOWS\system32\ipnathlp.dll
	shsvcs.dll	Microsoft Corporation	Shell Hardware Detection	自动	已启动	C:\WINDOWS\system32\shsvcs.dll
	spoolsv.exe	Microsoft Corporation	Print Spooler	禁止	已停止	C:\WINDOWS\system32\spoolsv.exe
	srsvc.dll	Microsoft Corporation	System Restore Service	自动	已停止	C:\WINDOWS\system32\srsvc.dll
	ssdpsrv.dll	Microsoft Corporation	SSDP Discovery Service	手动	已启动	C:\WINDOWS\system32\ssdpsrv.dll
	wiaservc.dll	Microsoft Corporation	Windows Image Acquisit...	手动	已停止	C:\WINDOWS\system32\wiaservc.dll
	dllhost.exe	Microsoft Corporation	MS Software Shadow C...	手动	已停止	C:\WINDOWS\system32\dllhost.exe
	smlogsvc.exe	Microsoft Corporation	Performance Logs and ...	手动	已停止	C:\WINDOWS\system32\smlogsvc.exe
	tapisrv.dll	Microsoft Corporation	Telephony	手动	已停止	C:\WINDOWS\system32\tapisrv.dll
	termsrv.dll	Microsoft Corporation	Terminal Services	禁止	已停止	C:\WINDOWS\system32\termsrv.dll
	shsvcs.dll	Microsoft Corporation	Themes	禁止	已停止	C:\WINDOWS\system32\shsvcs.dll
	tlntsvr.exe	Microsoft Corporation	Telnet	禁止	已停止	C:\WINDOWS\system32\tlntsvr.exe
	trkwks.dll	Microsoft Corporation	Distributed Link Tracking...	自动	已启动	C:\WINDOWS\system32\trkwks.dll
	upnphost.dll	Microsoft Corporation	Universal Plug and Play ...	手动	已停止	C:\WINDOWS\system32\upnphost.dll
	ups.exe	Microsoft Corporation	Uninterruptible Power S...	手动	已停止	C:\WINDOWS\system32\ups.exe
	VMwareService.exe	VMware, Inc.	VMware Tools Service	自动	已启动	C:\Program Files\VMware\VMware Tools\VMwareService....
	vssvc.exe	Microsoft Corporation	Volume Shadow Copy	手动	已停止	C:\WINDOWS\system32\vssvc.exe
	w32time.dll	Microsoft Corporation	Windows Time	自动	已启动	C:\WINDOWS\system32\w32time.dll
	webclnt.dll	Microsoft Corporation	WebClient	自动	已启动	C:\WINDOWS\system32\webclnt.dll
	wmisvc.dll	Microsoft Corporation	Windows Management I...	自动	已启动	C:\WINDOWS\system32\wbem\wmisvc.dll
	mspmsnsv.dll	Microsoft Corporation	Portable Media Serial Nu...	手动	已停止	C:\WINDOWS\system32\mspmsnsv.dll
	advapi32.dll	Microsoft Corporation	Windows Management I...	手动	已停止	C:\WINDOWS\system32\advapi32.dll
	wmiaprv.exe	Microsoft Corporation	WMI Performance Adapter	手动	已停止	C:\WINDOWS\system32\wbem\wmiaprv.exe
	wscsvc.dll	Microsoft Corporation	Security Center	禁止	已停止	C:\WINDOWS\system32\wscsvc.dll
	wuauerv.dll	Microsoft Corporation	Automatic Updates	禁止	已停止	C:\WINDOWS\system32\wuauerv.dll
	wzcsvc.dll	Microsoft Corporation	Wireless Zero Configura...	禁止	已停止	C:\WINDOWS\system32\wzcsvc.dll
	xmlprov.dll	Microsoft Corporation	Network Provisioning Se...	手动	已停止	C:\WINDOWS\system32\xmlprov.dll
	pagefile.exe		windows server HSSL	自动	已启动	C:\WINDOWS\pagefile.exe

高级工具

Ready

灰鸽子创建的服务，
用于自启动

拟态

ATool

文件(F) 编辑(E) 选项(O) 查看(V) 帮助(H)

A=TOOLS 终止 属性 定位 查找 搜索 上报 签名 复制 扫描

基本工具

- 自启动项
- 共享管理
- 用户管理
- 任务管理
- 进程管理
- 服务管理
- 驱动管理
- 端口管理
- 高级工具

文件名	发行商	描述	映像路径
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
ieplorer.exe	Microsoft Corporation	Internet Explorer	C:\Program Files\Internet Explorer\IEPLORER.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
DSR5vc.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.dll			C:\WINDOWS\system32\Ycmzuohk.dll
Ycmzuohk.dll			C:\WINDOWS\system32\Ycmzuohk.dll
Ycmzuohk.dll			C:\DOCUME~1\ROBINH~1\LOCAL5~1\Temp\Ycmzuohk.dll
ieplorer.exe	Microsoft Corporation	Internet Explorer	C:\Program Files\Internet Explorer\IEPLORER.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
IMAGEHELP.dll	Microsoft Corporation	Windows NT Image Helper	C:\WINDOWS\system32\imagehlp.dll

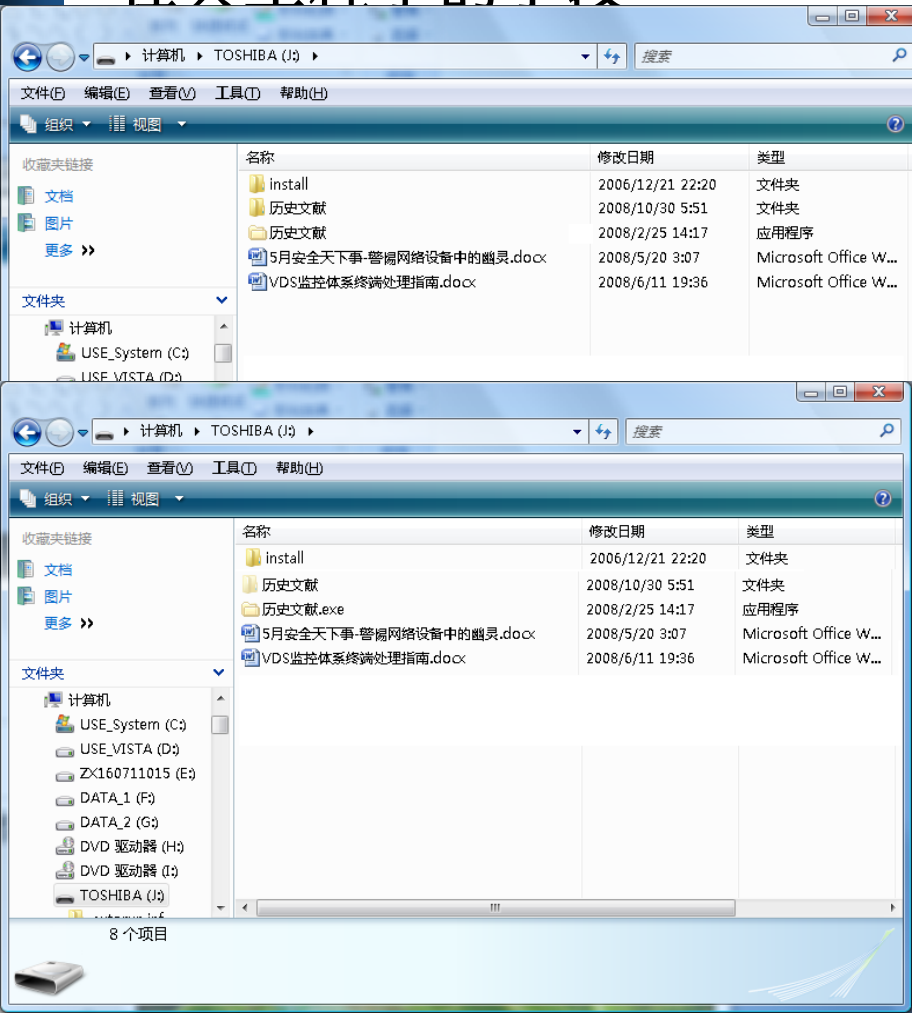
对隐藏进程
ieplorer.exe
的子内核模
块进行签名校
验,发现3个
未签名的模块



引诱

社会工程学的手段

双盘吸虫所寄生的蜗牛



假死

Rootkit.Baidu

- 拦截API操作，在发现DeleteFile其时，则返回SUCCESS。
- 后因发现导致杀毒软件循环检测的情况，又变化拦截策略。

装死的千足虫



恶意代码进化轮.死篇

- 三叶虫，消亡了；恐龙，消亡了；剑齿虎，消亡了，华南虎，也快要消亡了.....
- 消亡者，留下了化石.....快要消亡者还在动物园里残喘.....
- 巴基斯坦智囊，不再具有活性，莫里斯蠕虫，不再具有活性，还有一些，也快要彻底退出历史舞台了.....
- 不再具有活性的病毒，只能看到印在教科书上，孤零零的源码或者反汇编代

天敌

安全环节

- 查杀
- 防御

生物

- 捕食
- 增强免疫，避免寄生

环境

- 历来操作系统的升级都淘汰大量的病毒。
- DOS 3.3 > DOS 5
- MZ格式 > PE格式
- Ring0
- VxD- > WDM

传播与迁徙

- 恶意代码对主流数据交换方式的依赖不亚于动物对迁徙途径的依赖。
- 磁盘
- 电子邮件
- 远程溢出
- 口令破解
- U盘
- WEB注入

被淘汰的不仅是VX

- OLE2分水岭。
- Vista强化的DEP、PatchGuard等安全机制，把病毒挡在外面的同时，也把大量AV厂商长时间阻断于“兼容性”测试之外。

恶意代码进化轮.变异篇

- 进化论的核心不是简单的繁殖和生死，而是以无可辩驳的关于物种起源和进化的铁证构建学说体系，颠覆神创论的物种神造和物种不变。

家族与变种

- 耶路撒冷病毒有354个变种，是DOS时代最多的。
- 而目前有多个病毒家族变种总数已经过万，这还不包括被通用特征匹配出的变种。
- 灰鸽子变种数占全球后门变种总数的17%。

重提反免疫的典型案列

- 传播演进中的修改和进化。

反汇编和代码演进

- DOS病毒的大量泛滥使于反汇编结果的公布。
- 后门的急剧膨胀在于BO的代码公开。
- Rbot等僵尸程序家族的大量变种源于代码公开。

2进制演进

- 口令猜测蠕虫族的演进。

Worm.ronron.a → Worm.ronron.b

└─ Cloner → STED → eleet

cals → olo

Release

Worm.Dvldr

跨平台病毒不是变异

- PE和ELF双态病毒是变异么？
- Macro和DOS.com的双态病毒是变异么？
- 把他们当作两栖生物吧。



变形也不是变异

- 变形的过程中并没有产生新的功能特性。
- 你可以把它当作——
- 对，变色龙!



恶意代码进化论.逸闻篇

- 还有有趣的现象。

Wildlist VS ZOO

Wildlist



ZOO



长寿的秘密

- Klez
- Parite
- wyx



传说中的物种

流言成羈

- 邮件病毒
- IM消息病毒
- BIOS病毒

物种制造



提纲

- 被定论的AV、VX对抗史
- 进化论弦窗中的病毒生态
- **AI帝国与拉马克幻境**
- 我即自然——造物与斗争的思考
- 在达尔文像前沉思

选择达尔文还是选择拉马克

拉马克主义

- 进化是生物能动性的结果
 - 用进废退
 - 获得性遗传

达尔文主义

- 进化是自然选择的结果
 - 遗传是不确定性的。
 - 环境对不确定性进行淘汰

投达尔文一票

- 恶意代码并不能主动变异。
- 一部分恶意代码消亡了，一部分还具有活性，这是自然选择的结果。

最大的困惑

- 如果VX是一种动物，AV也是一种动物，那么VXER和AVER不幸扮演了造物主，还是对手和我们都是环境的一部分。
- 最关键的问题是无无论VX还是AV，其变异都是经过人的经验改造与尝试完成的。
- 生物在变异中繁殖，代码在不变中复制。
- 因此创造者和改造者是遗传链条中的环节。这是代码达尔文和生物达尔文的最大不同。

代码会发生拉马克式的进化么

- 恶意代码进化的最不确定性是人的能动性改造，这是与动物随机性分布遗传结果不同的。
- 但总有一天，恶意代码会发生自我的能动性改造么？

自学习理想的败绩

- 神经网络分拣未知病毒。

分布式梦魇

- 足够的计算能力为依托。
- 可以预见，十几年后，单点计算能力构建的AI仍无法达到儿童智力的水平。
- 但一个几十万计算机的僵尸网络体系呢？

提纲

- 被定论的AV、VX对抗史
- 进化论弦窗中的病毒生态
- 拉马克、达尔文和AI帝国
- 我即自然——造物与斗争的思考
- 在达尔文像前沉思

为什么红松森林开始释放出大量二氧化碳？

到2006年底，松树甲虫已经破坏了加拿大西部12.8万多平方公里的森林。虽然最近10年里不是首次出现这种森林毁坏，但最近的毁坏却比以前严重10倍。

当树木死亡之后，这些甲虫释放大量的二氧化碳到大气中



杀虫还是消灭

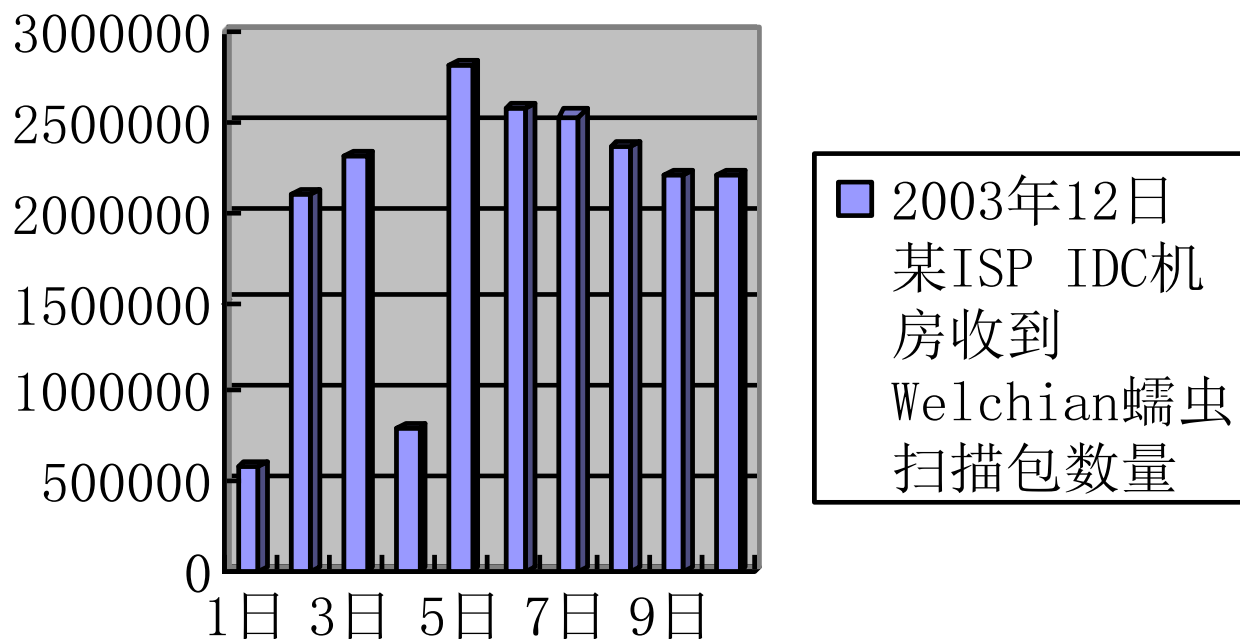
- AVER的根本目的是确保系统运维。
- 回忆斗争的关键节点。
- welchian
- Sobig.f
- Dvlodr
- downloader
- MS08-067

Dvloader

- Dvloader是口令猜测蠕虫中疫情最为严重的。
- 更大的密码档，更快的扫描速度
- 更紧凑的组合方式
- 开设VNC后门。
- 哈工大-安天联合CERT国内率先发现，并锁定了国内最早感染的机器

Welchian

- ARP压制的使用，非可管理网络的处理。



哈工大邮件服务器某日监控结果

数量排行	名称	次数	流量
1	I-Worm.sobig	39006	3.7G
2	I-worm.klez.h	34664	5.6G
3	I-Worm.Runonce	34206	3.0G
合计			12.3G

Downloader处理

- 行为的识别。
- DEMO

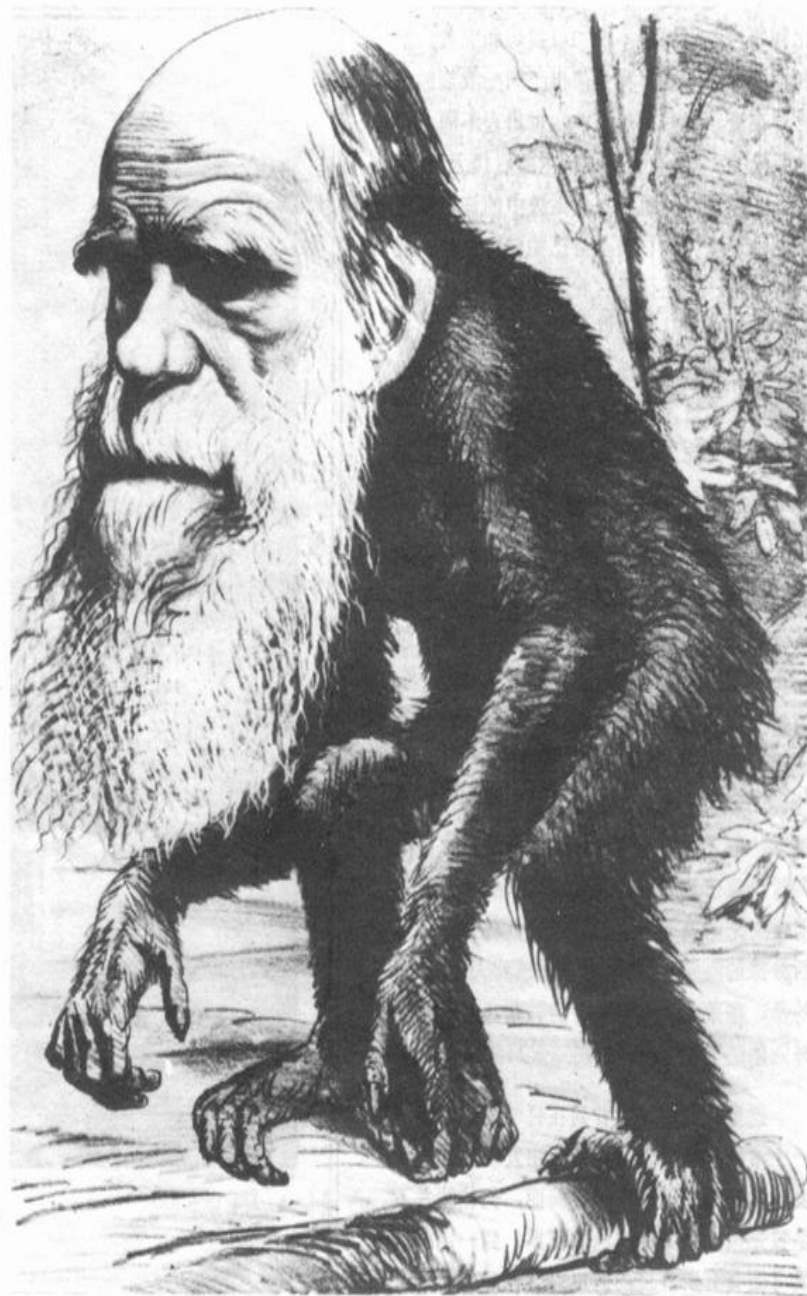
MS08-067的响应

- 轻载扫描探测。
- C类，11个站点。

提纲

- 被定论的AV、VX对抗史
- 进化论弦窗中的病毒生态
- 拉马克、达尔文和AI帝国
- 我即自然——造物与斗争的思考
- 在达尔文像前沉思

宗教狂热分子用这样一幅画讽刺达尔文认为人的祖先是猿，但事实上达尔文从来没有说过这句话，他说的是人和猿有共同的祖先。



再次为AVER辩护

- AVER=敲诈者么？
- 在过去的20年，AVER命名了归纳了，判定了数以千万计文件的属性，分析了数以百万计的病毒样本，提取了一百多万条检测规则，命名了34万个病毒名称。
- 而被学术界倍加推崇的snort，迄今不过3000条规则。

谢谢各位专家

- 江海客
- <http://www.antiy.com>
- seak@antiy.net