# 木马测试分析报告

报告编号：HJ_test_ztgame_muma01

木马测试载体：征途资料片世外桃源

上海征途网络科技有限公司

## 文档信息

| |
|---|
| **标题：** 征途木马测试分析文档 |
| **作者：** 魏春雷 |
| **创建日期：** 2007-4-4 |
| **上次更新日期：** 2007-4-6 |
| **版本：** 1.2 |
| **部门名称：** 测试部 |

## 修订文档历史记录

| 日期 | 版本 | 说明 | 作者 |
|---|---|---|---|
| 2007-4-4 | 1.0 | 新建，信息搜集 | 魏春雷 |
| 2007-4-5 | 1.1 | 木马测试 信息记录 | 魏春雷 |
| 2007-4-6 | 1.2 | 问题分析 文档汇总 | 魏春雷 |

# 一、 概述

## 1 编写目的

编写本木马测试报告的目的是为软件开发项目管理者、质量测试管理者、公司领导、征途用户提供关于木马盗取用户用户名密码功能的测试记录、测试结果和测试分析。

## 2 项目背景

针对目前常见征途的盗号木马进行测试分析其发作原因，并且提出合理化建议，以及防治木马的必要手段。计算机一旦感染到这些木马，就有可能被执行文件操作、注册表操作、键盘记录等任意网络操作。最后极有可能导致游戏帐号、虚拟物品丢失，给玩家带来损失，给游戏公司带来损失。

## 3 术语和缩写词

征途: 征途资料片世外桃源

木马: 征途木马

Fx: Trojan.PSW.ZhengTu.fx 征途木马变种 FX

Xo: Trojan.PSW.ZhengTu.xo 征途木马变种 XO

gz: 灰鸽子 2007

# 4 参考资料

测试报告模板

征途官方网站

黑客木马网站

# 二、 测试概要

此木马测试分析报告针对征途搜集木马，对所搜集到的 2 种征途密码发送变种木马、1 种远程控制木马进行相关功能的测试，从而发现其传播途径，攻击手段，并且给出预防措施，以及预防建议。有效防止公司、玩家受到损害。2 款杀毒软件以及实时监控对木马的遏制能力。以及游戏本身对木马程序的免疫能力。

# 1 测试用例设计

关闭防火墙杀毒软件

开启 P2P 终结者（也可用其他软件监测） 抓包检测 网络数据流向。

每一用例结束后使用杀毒软件或专杀工具清除原木马修复注册表启动项后进行下步测试。

| 测试编号 | 测试内容 | 输入 | 预期结果 | 实际结果 |
|---|---|---|---|---|
| Tszt01 | Fx/xo 对游戏帐号的拦截 | 启动木马，进入征途，输入帐号后键盘输入密码。 | 帐号、密码被拦截并且发送到制定邮箱 | 同 预期 |
| Tszt02 | Fx/xo 对软键盘输入密码的拦截 | 启动木马，启动征途，使用软键盘输入密码 | 帐号、密码被拦截并发送到制定邮箱 | 密码未被拦截 |
| Tszt03 | Fx/xo 对二级密码的拦截 | 使用财产保护，输入密码 12345678 | 二级密码被拦截发送到指定地址 | 同 预期 |
| Tszt04 | Gz 绑定后传播,对用户电脑的控制 | 启动 GZ 客户端 | 注册表被感染、并在系统目录下释放 G_Server.exe、G_Server.dll 和 G_Server_Hook.dll | 同 预期 |
| Tszt05 | Gz 对征途的密码拦截 | 启动征途，输入密码，登陆。进行游戏。 | 可以看到用户的一切操作，对测试机拥有最高权限。 | 同 预期 |

分别启动杀毒软件卡巴斯基，金山毒霸。

| 测试编号 | 测试内容 | 输入 | 预期结果 | 实际结果 |
|---|---|---|---|---|
| Tszt11 | 电脑内的Fx/xo,杀毒软件对Fx/xo的处理情况 | 启动木马，杀毒软件报警，并提示是否清除木马。 | 木马被清除 | 同预期 |
| Tszt12 | 网络上的Fx/xo杀毒软件实时监控对其处理情况 | 打开带有Fx/xo的网页，杀毒软件报警，并提示是否阻止。 | 木马被阻挡在防火墙外 | 同预期 |
| Tszt13 | 下载带有Fx/xo的软件，杀毒软件是否有效发现 | 下载带有fo/xo的征途外挂，下载后，杀毒软件检查并提示清除木马。 | 下载后自动检查，并且提示清除木马或者删除文件。 | 同预期 |
| Tszt14 | 接受与图片绑定的gz,杀毒软件是否有效发现 | 利用QQ传送已经与gz绑定的征途图片 | 传送后杀毒软件，杀毒软件并不检查文件。 | 同预期 |
| Tszt15 | 已经被gz入侵,杀毒软件对文件的处理 | 使用杀毒软件进行全盘扫描 | 有效清除gz文件 | 同预期 |
| Tszt16 | 已经被gz入侵,杀毒软件对注册表的处理 | 使用杀毒软件进行全盘扫描 | 有效修复被感染注册表 | 并不能有效修复注册表被窜改文件 |

# 2 测试环境与配置

测试产品：征途资料片世外桃源 木马

软件环境：Microsoft Windows XP Professional

版本：5.1.2600 Service Pack 2

卡巴斯基反病毒软件 6.0

版本：2007-4-5 7:29:33

金山毒霸 2007

病毒库版本：2007.4.4.17

P2P 终结者 2.07

Trojan.PSW.ZhengTu.fx

Trojan.PSW.ZhengTu.xo

灰鸽子 2007

硬件环境：个人电脑 CPU:Celeron(R)2.66GHz

内存:512MB

虚拟内存：1G

显卡:ATI RADEON 9550

硬盘：160G 系统区空间 15G 可用空间 10G

征途安装区空间 30G 可用空间 20G

网络环境：歌华有线宽带 上行 10K 下行 100K

## 3 测试方法

此次主要是对木马功能的测试包括发送信息的获取，信息包括用户名，密码，二级密码，数字密码信息，以及杀毒软件对木马的处理，以手工方式测试并搜集相关木马更新服务器。

# 三、 测试结果及缺陷分析

## 1 测试执行情况与记录

使 2 台测试机保持相对孤立，切断其在局域网内与其他计算机的联系。

2 台测试机进行木马传送。

每个用例执行后清除病毒。

测试结束后对 2 台电脑进行全面木马检测，查杀病毒。

## 2 测试组织

参与测试人员：魏春雷

# 3 测试时间

| | | |
|---|---|---|
| Fx | 2007-4-5 | 09：00－12：00 |
| Xo | 2007-4-5 | 13：00－16：00 |
| gz | 2007-4-5 | 16：00－22：00 |
| gz | 2007-4-6 | 09：30－18：00 |

# 4 测试版本

Fx xo gz2007 变种

# 5 木马的统计与分析

Windows 的漏洞比较多，不单可以通过木马侵入用户计算机，还可以通过系统漏洞侵入系统，控制用户计算机，窃取用户资料。

征途最新发现的高危险 ANI 鼠标指针漏洞，该漏洞非常严重，危害面积非常广！

已有大量木马、恶意程序、蠕虫病毒使用该漏洞进行传播,绝大多数反病毒软件、防漏洞软件、主动防御软件失效！

必须更新 XP 最新补丁 WindowsXP-KB925902-x86-CHS 遏止其传播。

由于时间仓促只对密码发送木马和远程控制木马做了比较浅显的测试及分析

密码发送木马一旦被执行,木马会记录受害者的键盘敲击并且在

LOG 文件里查找密码，自动搜索内存，Cache，临时文件夹以及各种敏感密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱。从而达到获取密码的目的，所以这类木马大多使用 25 号端口发送 E-mail。大多数这类的木马不会在每次 Windows 重启时重启。这种特洛伊木马的目的是找到所有的隐藏密码并且在受害者不知道的情况下把它们发送到指定的信箱，如果体育隐藏密码，这些特洛伊木马是危险的。

远程控制木马，此木马的危害性及其严重，它是各种木马的杂和体。可以说这种木马的危害程度超越了其他种类木马数倍。一身间具各种木马的能力，是木马中的王牌。中了此种木马控制这在操作被控制机时犹如在自己的电脑上操作一样。

如以上二种还有破坏型的木马、DOS 攻击型木马、反弹端口型木马、程序杀手型、代理木马、FTP 木马等诸多类型。

木马重要是通过网络传播的，所以网页，外挂，软件下载等可以直接被用户使用的元素成为木马传播的主要途径。木马越来越变化多端，加密自身，规避杀毒软件甚至是令防病毒软件失效，隐藏自身。是使清除木马造成一定的困难，所以要在木马进入用户系统之前遏止它。

用户不能利用手上的现有手段对付木马，这也是木马猖獗，使用户蒙受损失的一个弊病。

# 四、 测试结论与建议

## 1 测试结论

由于时间仓促此次测试并不充分，对系统的漏洞，杀毒软件，木马种类的搜集并不全面，无法做出更加具体详尽的测试。

相对于杀毒软件可以随时更新到最新版本。不过新型病毒总是先出现，杀软才能更新。

系统补丁重中之重，不过和杀毒软件一样也处在比较被动的位置。

所以防御手段只能靠个人主动防护，有一定的安全意识。

## 2 建议

建立良好的安全习惯，不打开可疑邮件和可疑网站;

很多病毒利用漏洞传播，一定要及时给系统打补丁;

安装专业的防毒软件升级到最新版本，并打开实时监控程序;

安装带有“木马墙”功能的个人防火墙软件，防止密码丢失;

不接受陌生人传送的文件;

下载文件后一定要查杀病毒，木马。

# 五、 游戏保密措施相关截图