



**ThreatScape eCrime**™

Security beyond the edge

# 中国的“网银大盗”分析

2009年06月06日

# 中国的“网银大盗”分析

## 综述

中国第一个被称为“网上银行盗贼（网银大盗）”的网上银行木马于 2004 年 4 月公布于众。此后，犯罪分子通过电脑病毒对网上银行账户进行攻击盗窃的犯罪案例开始屡见不鲜。自 2004 年至 2008 年，网上银行盗窃形式开始不断繁衍变化。目前，个人及公司网上银行账户由于受到网上银行木马攻击而被盗的案件一直不断增加，严重影响了中国网上银行业务的健康发展。最开始，网银大盗将目标定位于盗窃银行卡，但随着攻击代码自身的发展成熟，这些犯罪分子的犯罪目标也更加多样化。

## 网银大盗团伙

网银大盗团伙在研发、传播和销售网上银行木马程序时隐蔽得几乎无从追拿，并且中国执法机构对于他们的个人身份和作案习惯也知之甚少。到目前为止，能够与他们进行联系或直接沟通的唯一方式就是通过购买其产品和服务，例如：定制服务或所谓的“特别项目”等。尽管近几年来网上银行盗窃团伙层出不穷，但到目前为止，还没有一个盗窃团伙能够像网银大盗团伙那样执著和专业。

该团伙不断研究新代码并对木马进行升级，他们的行为已经严重影响了公众对中国网银系统的信任度。虽然执法机构已多次尝试抓捕该团伙，但是该团伙仍在不断地升级版本，目前最新版本被称为“网银大盗 1.7”。该团伙不同于其他犯罪团伙，非常专业并且组织严密。他们的研究和开发都在内部进行，而且在网上信息板和公告栏上有很多人反映，该团伙要求购买者要达到他们提出的技术上的要求以确保其产品得到合理的使用，否则将拒绝出售。目前该团伙被执法机构和独立研究人员视为网银系统最直接且最致命的威胁组织。

## 网银大盗现状

1. 被感染的用户数量快速增加。自 2004 年 8 月至 2008 年 10 月，中国被感染病毒的用户数量比以往增加了 6 倍。与此同时，银行卡盗窃案件常有发生，涉案金额从 1 万元到数百万元不等。
2. 盗窃技术不断改进升级。以前的网上银行盗窃行为都是瞄准那些账户名和密码过于简单的用户，现在连具有数字证书的用户也已经成为被攻击的目标。

网上银行木马技术随着病毒的繁衍变化而不断发展。早期木马攻击是通过键盘监视来盗取用户的账户名和密码。随着一些银行开始使用软键盘来抵御木马攻击，木马制造者又向木马中添加了数字图形捕获功能。许多银行已意识到用户在使用账户名和密码登

录时所存在的风险，并开始限制那些用户的交易金额，所以目前更多的网银木马开始将攻击目标定位于具有电子证书的用户。

## 网银大盗攻击方法

根据网上银行木马的技术原理，目前攻击网上银行账户的方法包括以下几种类型：

- 1、键盘监视：**这是网上银行木马普遍采用的盗取方式。它在后台运行并监视用户的浏览器，一旦用户登录了网上银行的登陆网页或支付网页，用户键盘上输入的信息就会被它用“钩子技术”记录下来，然后通过电子邮件把盗取的账号和密码寄给犯罪分子。
- 2、数字图形捕获：**这是盗取账户信息的另外一种技术。当被监视的用户访问网上银行的网页时，木马就会复制（或记录）该网页的屏幕信息。由于采用高效的数据压缩技术，一些木马可以将一分钟的屏幕信息压缩成一个只有几百个千字节的文件。
- 3、数字证书盗窃：**最新的网银大盗能够盗取用户的数字证书。攻击者能够通过该木马对被入侵的电脑进行远程控制并获取数字证书。另外，中国大多数的银行使用 IE 数字证书系统来管理自己的证书文件，所以该木马可以通过 Windows 下的编程接口来盗取数字证书。
- 4、浏览器嵌入：**也被称作“浏览器劫持”。部分木马的源代码被嵌入了浏览器中，每当浏览器运行时，那些源代码也随之运行。一旦这些恶意代码被嵌入到浏览器，那些敏感数据会在被浏览器加密前就提前被木马捕获。
- 5、网络钓鱼：**通过伪装成一个真实的网上银行的网页或网上商店的网页来诱骗用户输入个人信息，如银行帐号和密码。过去，攻击者通常是通过发送电子邮件诱骗用户访问虚假网页，但现在银行卡用户比以往更加警觉，所以攻击者使用网上银行木马进行窃取并通过一些技术手段来隐藏自己的不法行径，例如伪造一个弹出窗口或更改地址等。通常情况下，网银窃贼往往综合以上多种手段来更迅速更有效地盗取账户信息。

## 网银大盗源代码

“网银大盗 1.7”的源代码实际上是来自阿根廷的一个代码家族，该代码被网银大盗团伙购买并通过进一步修改后在中国应用。该代码所具有的拉丁美洲属性被全部清除，并被修改成只有在汉语系统下才能工作。埃赛特伙伴公司于 2009 年 4 月 17 日经可靠渠道证实了上述代码的情况。

发现该源代码的产地蕴含了很多含义，最重要的就是此恶意代码已经发展成为一个跨区域性

传播的代码，并且将不断地升级更新。虽然该代码源于拉丁美洲，但已经应用于中国，并很可能向东亚和北美传播扩张。埃赛特伙伴公司将继续与拉丁美洲工作人员一同协作密切注视并研究该木马及其团伙的活动。

埃赛特伙伴公司经可靠渠道获得了“网银大盗 1.7”恶意代码并进行了研究，以便更好地帮助客户进行防范。该代码本身具有以下属性：

- 只在中文系统下进行工作
- 具有 rootkit 属性
- 具有键盘记录功能，并且能够被 URL 字符串匹配触发
- 具备盗取游戏账号的功能

网银大盗团伙除了提供网上银行木马程序，还提供解密服务、木马程序的定制化服务和分布式拒绝服务攻击。他们对于一个免费邮件解密的收费为 300 元，且承诺完成期限为两天。而攻击特定的服务器或网站，其收费要依据网站的知名度高低，攻击的难易程度及要求的受攻击程度而定。

该团伙的业务管理流程非常专业化，每一笔交易都有一个订单号，整个业务流程都有记录和编号，并提供相关的客户售后服务。

## 埃赛特评估

综上所述，中国网银犯罪团伙十分猖獗，分工明确、组织架构严密和业务流程专业化是其主要的特点。据埃赛特伙伴公司调查，一些犯罪分子已经将其目光转向了国外市场，同时以往的个体犯罪活动逐渐演变成一条完整的黑色产业链，并且其规模在不断的扩大，其中以网银大盗为代表的木马攻击占据了产业链极大部分。

埃赛特伙伴公司将继续密切注视并研究该木马及其团伙的活动。与此同时，埃赛特伙伴公司也将利用国内外的资源为该团伙锁定的国际受攻击对象提供更高级别的解决方案。