



**ThreatScape eCrime**™

Security beyond the edge



## “转移赃款服务”的新途径： 利用自动票据清算系统转移赃款

2008年10月21日

## “转移赃款服务”的新途径：利用自动票据清算系统转移赃款

### 综述

从俄罗斯黑客犯罪论坛上选摘的帖子中，一个说英文的名叫“elit3”的人，叫卖被侵账户的“更改账户地址和注册信息”服务，声称他有很多这样的“大通/花旗/第一资本/美联银行”的账号可以卖，价格按账号余额而定，余额为 1000-5000 美元价格为 100 美元（或等值的网络 WMZ 币），最高余额超过 15000 美元。(编者按：这只是“elit3”提供的三个服务中的第二个。他的第一个服务是根据信用卡号码提供信用卡的全部信息，他的第三个服务是提供社会保险号码/出生日期的搜索服务。)

```
2-Cobs/enrolls
come with same info as full info
with the exclusive mail access 📧
mostly chase/citi/cap1/wachovia

prices :
1-5k 100$ // 5-10k 150$ // 10-15k 200$ / 15k+ 250$ wmz
according to balance
mostly none of them has wire xfer enabled
but they can do ACH to external accounts if u have a method..

3-ssn/dob lookup service
search fields are
first name /last name address city state zipcode
then u click submit
it get you all possible results with addresses and phones
u can only put name and state if u need random results

# i create u username and password n give u url
#great uptime..

prices : contact me for it..
```

*"elit3"的更改账户地址和注册信息服务*

```
elit3 IS VERIFIED for US full info by bin, enrolls selling and ssn-dob lookup
service

Key ID: 0x627C163E
Fingerprint: 2A12 DAFF 4465 4C9C B100 789B 80B4 42B6 627C 163E

JabberID: obnon@ajabber.net

First contact in PM
Respect someone else's time
```

*"elit3"的三个服务被论坛管理员 Obnon 所证实  
(埃赛特伙伴公司资讯)*

“elit3”提供的服务也被该论坛管理员，在地下市场非常有名的“Obnon”所证实。在上面的第二个截屏图，“Obnon”确认了“elit3”在该论坛发布的所有服务的真实性，基本上是以该论坛的名义和声誉为他的三个服务做担保。

#### **埃赛特的评估：利用自动票据清算系统转移赃款**

“elit3”的第二个服务（第二张截图）最引人注目的是他说的关于更改账户地址和注册信息部分，他声称绝大部分类似的账号还没开通电汇转钱功能，但是可以通过自动票据清算系统（ACH）将钱转入其他账号。自动票据清算系统是一种利用电子资金进行汇兑的电子支付系统，所有的美国银行都在使用。埃赛特的专家注意到其他的俄罗斯犯罪分子，例如：“国会”（House[of]Parlament）和“阿莱克斯”（ajax\_c\_i）也使用 ACH 转移账款。“国会”声称喜欢使用 ACH；“阿莱克斯”说他在印度、智利、西班牙、葡萄牙、中国、新加坡、加拿大和马来西亚都有下家，接受电汇和在美国的非存款 ACH。

埃赛特伙伴公司将继续收集并报告 ACH 系统在非法市场的使用和发展情况。