A.

2013

50 4

12

SSL

…

B.

2013

2012 10 24 50

50

“ ”

50

1. SSL
2.
3.
4.
5. “
”
6.
7.
8.
9.

10.
11.
12.
13.
14.

15.
16.
17.

18. USBKEY
19.
20.

A. I
B. II
C. III
D. 1
D1. 1
1) SSL 2
2) 3
3) 6
4) 7
5) “ ” 7
6) 9
7) 9
8) 10
9) 10
D2. 12
10) 13
11) 14
12) 15
13) 16
14) 16
D3. 17
15) 18
16) 19
17) 20
D4. 21
18) USBKEY 22
19) 23
20) 23
E. 24

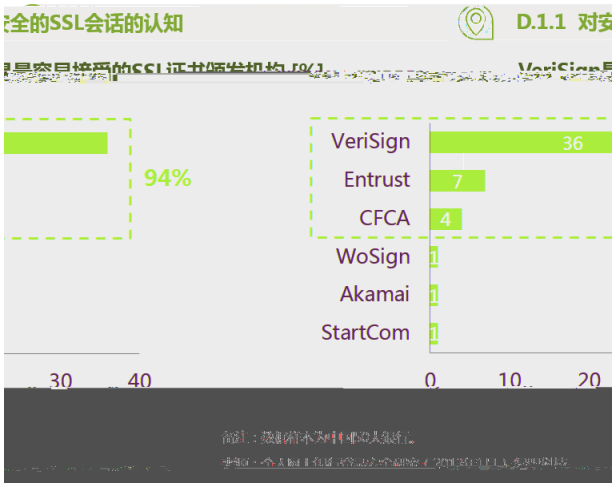
D.

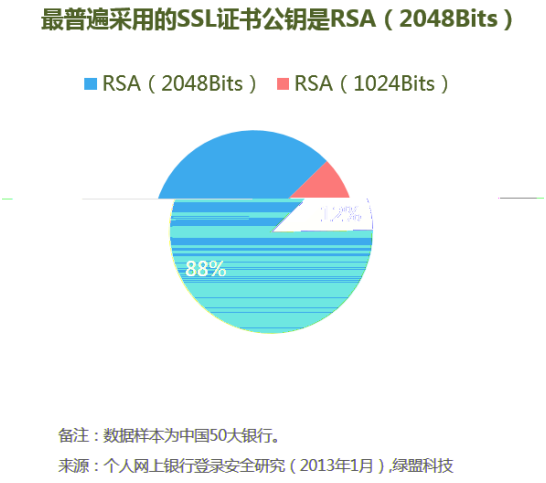
D1.

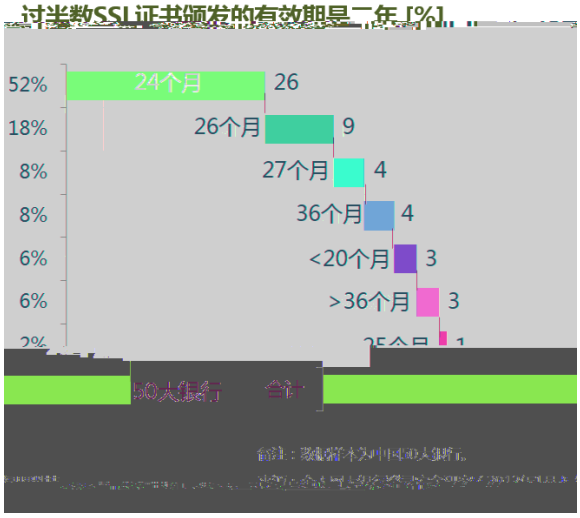
1) SSL

RSA 2048Bits RSA
1024Bits
50 24-27 9

HTTPS SSL
SSL
VeriSign D.1.1
SSL VeriSign Entrust CFCA





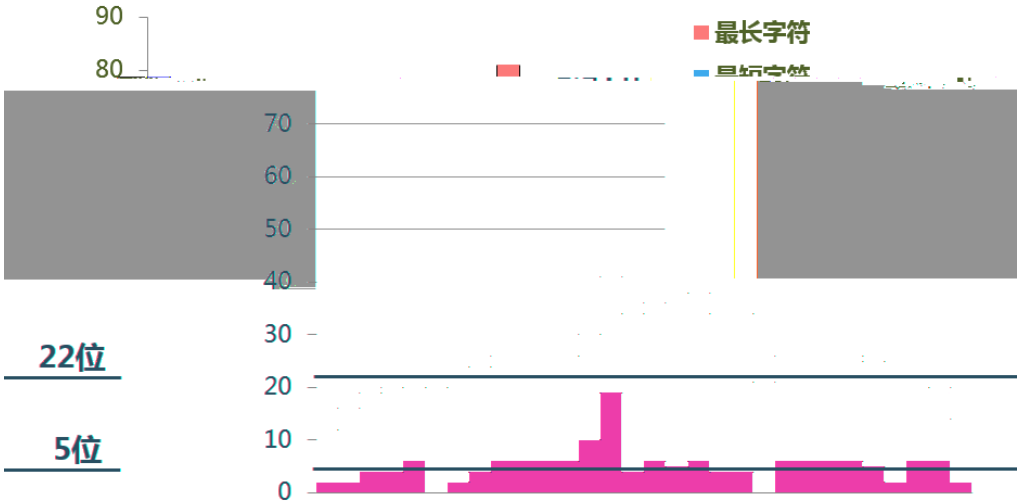


“ SSL SSL

”

D.1.5 用户名和密码的安全策略要求更加严格

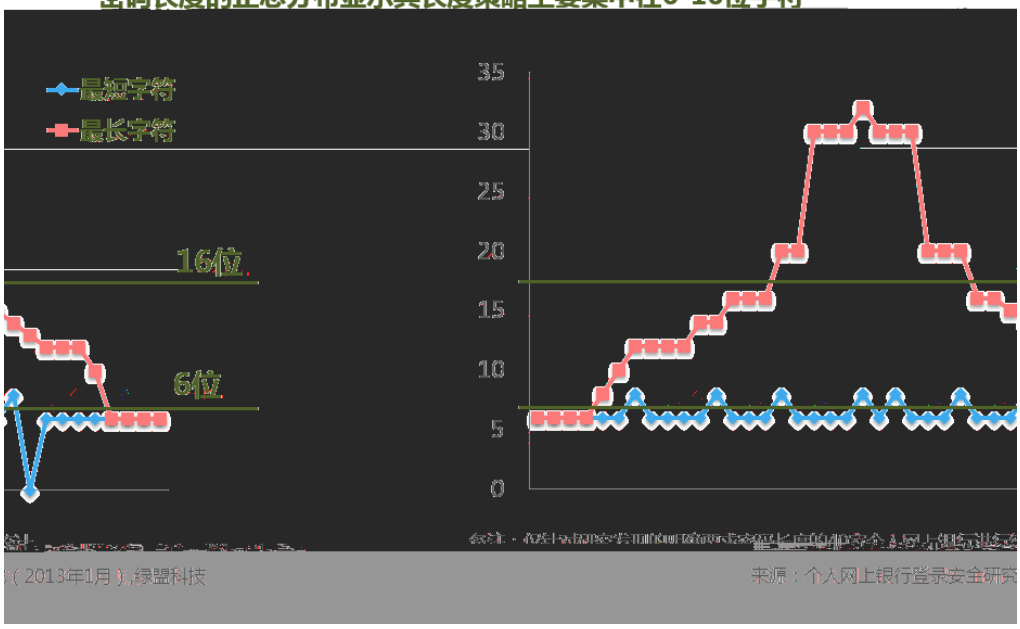
登录用户名长度的正态分布显示其长度策略主要集中在5-22位字符



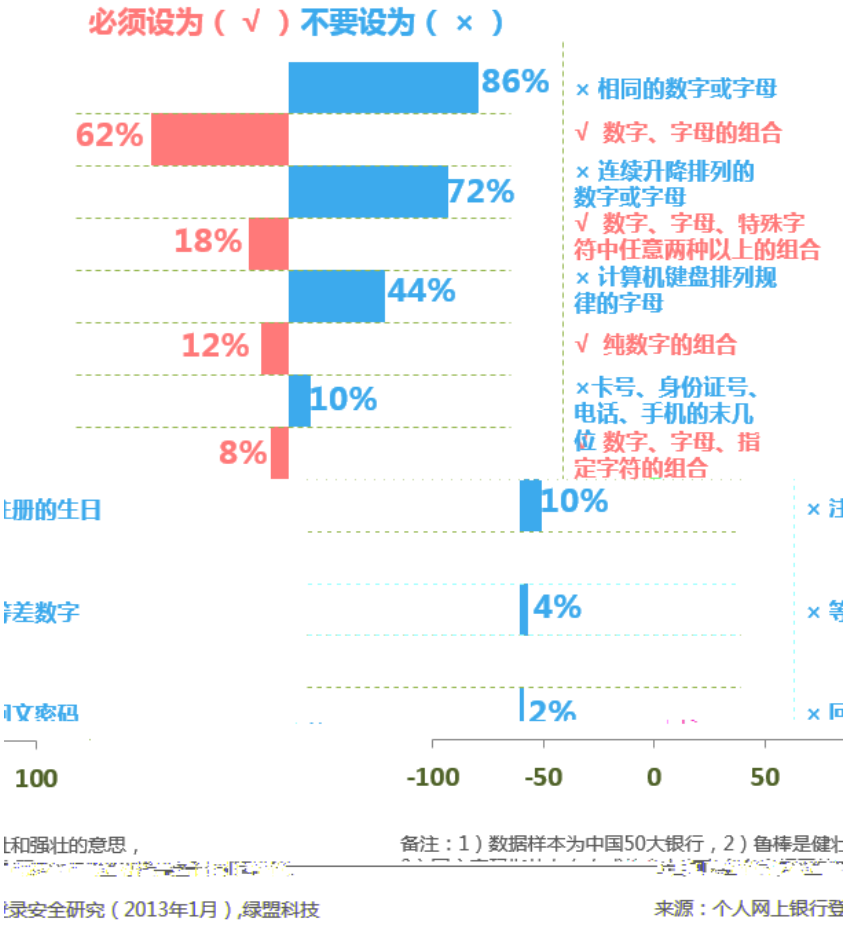
备注：仅针对研究发现的明确要求用户名长度的30家个人网上银行进行统计

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

密码长度的正态分布显示其长度策略主要集中在6-16位字符



D.1.6 密码复杂度策略是6-8位短密码实现强鲁棒性的必要保证



比和强壮的意思，　　备注：1）数据样本为中国50大银行，2）鲁棒是健壮

录安全研究（2013年1月），绿盟科技　　来源：个人网上银行登

3)

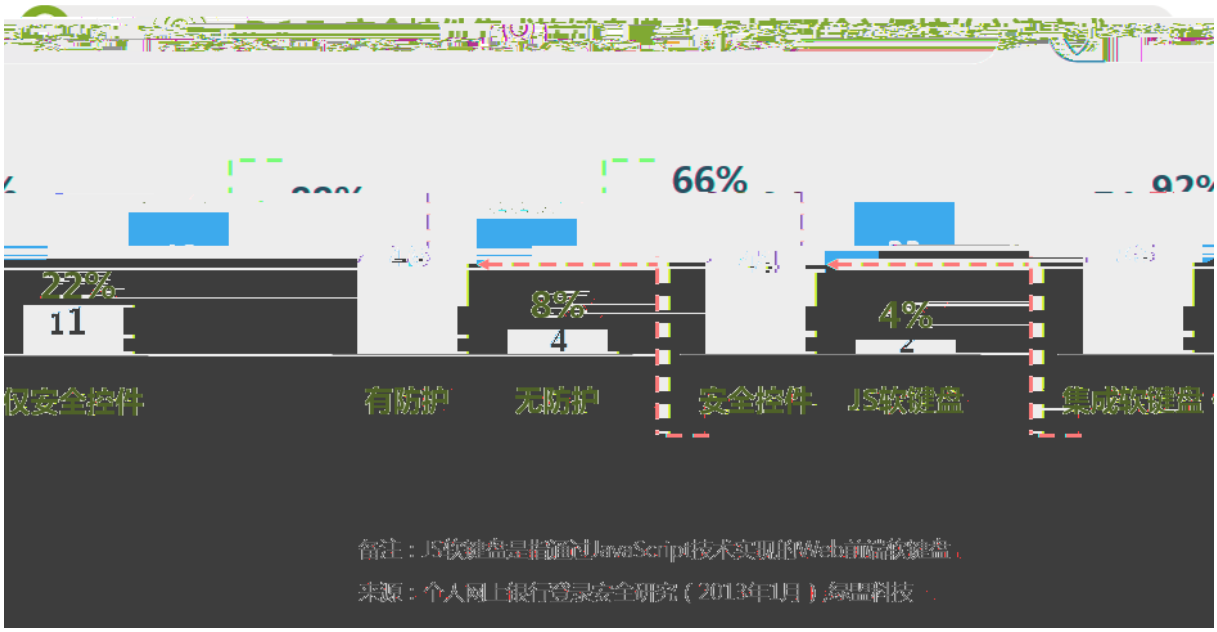
“ ”

“ ”

“ ”

86%

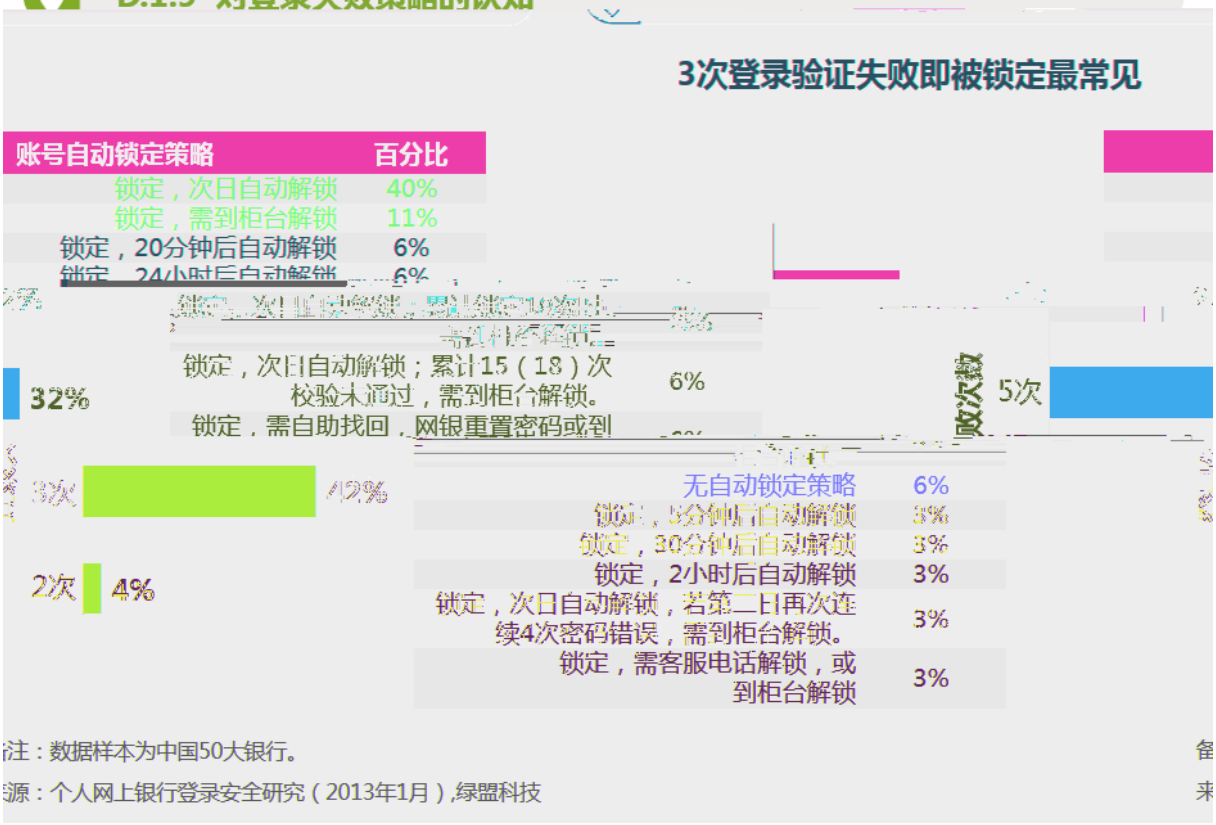
D.1.7


66%
27%
11
8%
4
4%
2
有防护
无防护
安全控件
JS软键盘
集成软键盘
备注：JS软键盘是指通过JavaScript技术实现的Web前端软键盘
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“

”

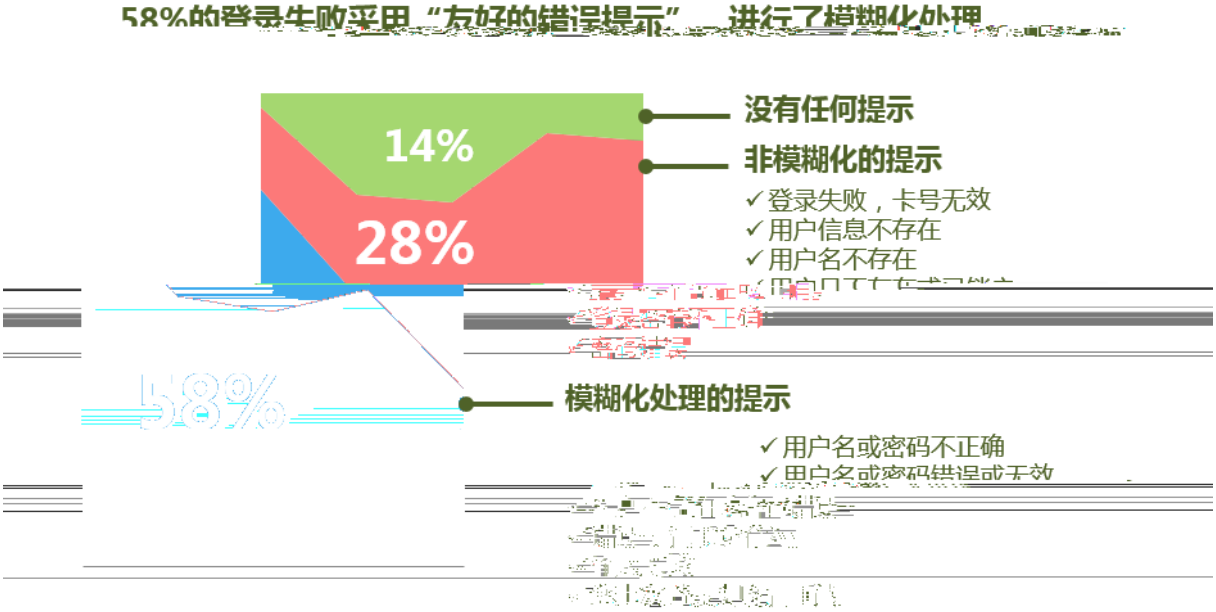
D.1.9 对登录失败策略的认知



注：数据样本为中国50大银行。

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

D.1.10 对登录失败后错误提示信息的认知



备注：数据样本为中国50大银行。

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

8)

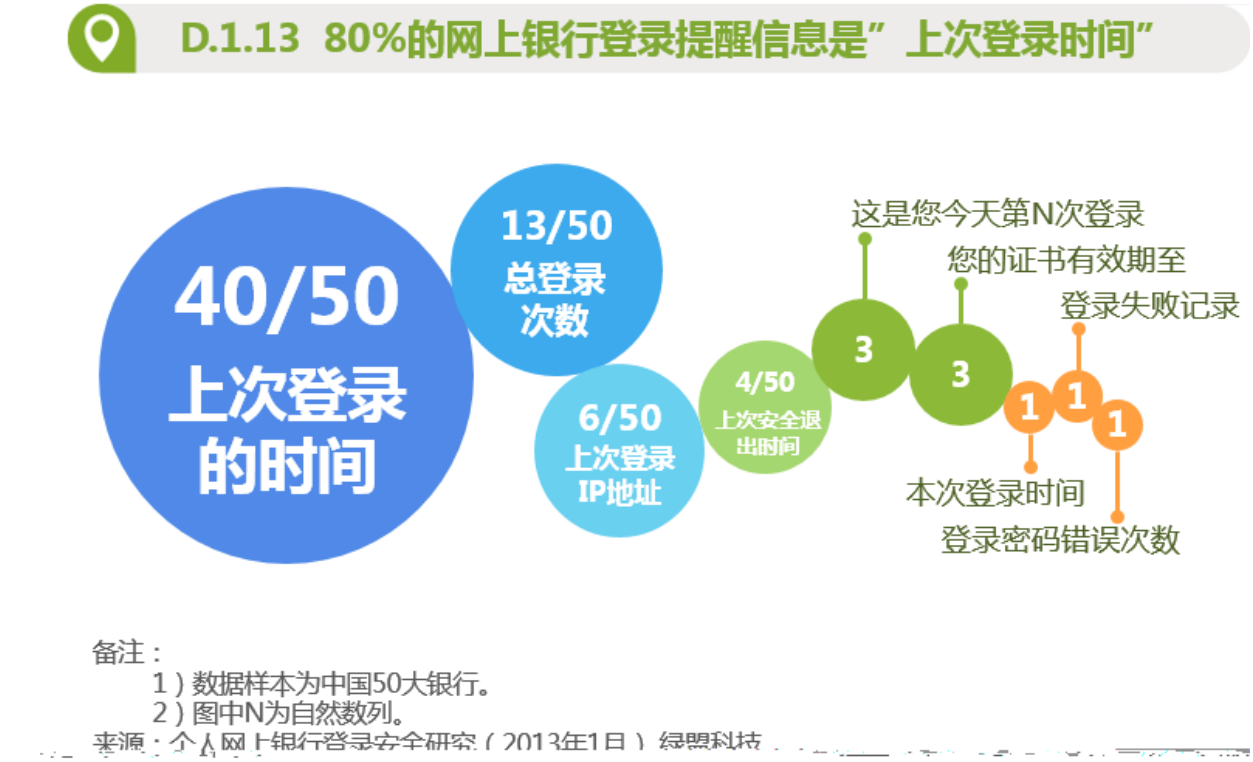
“

”

“ ” “ ” “

IP ” “ ” “

” D.1.13



9)

“ ” “ ” “

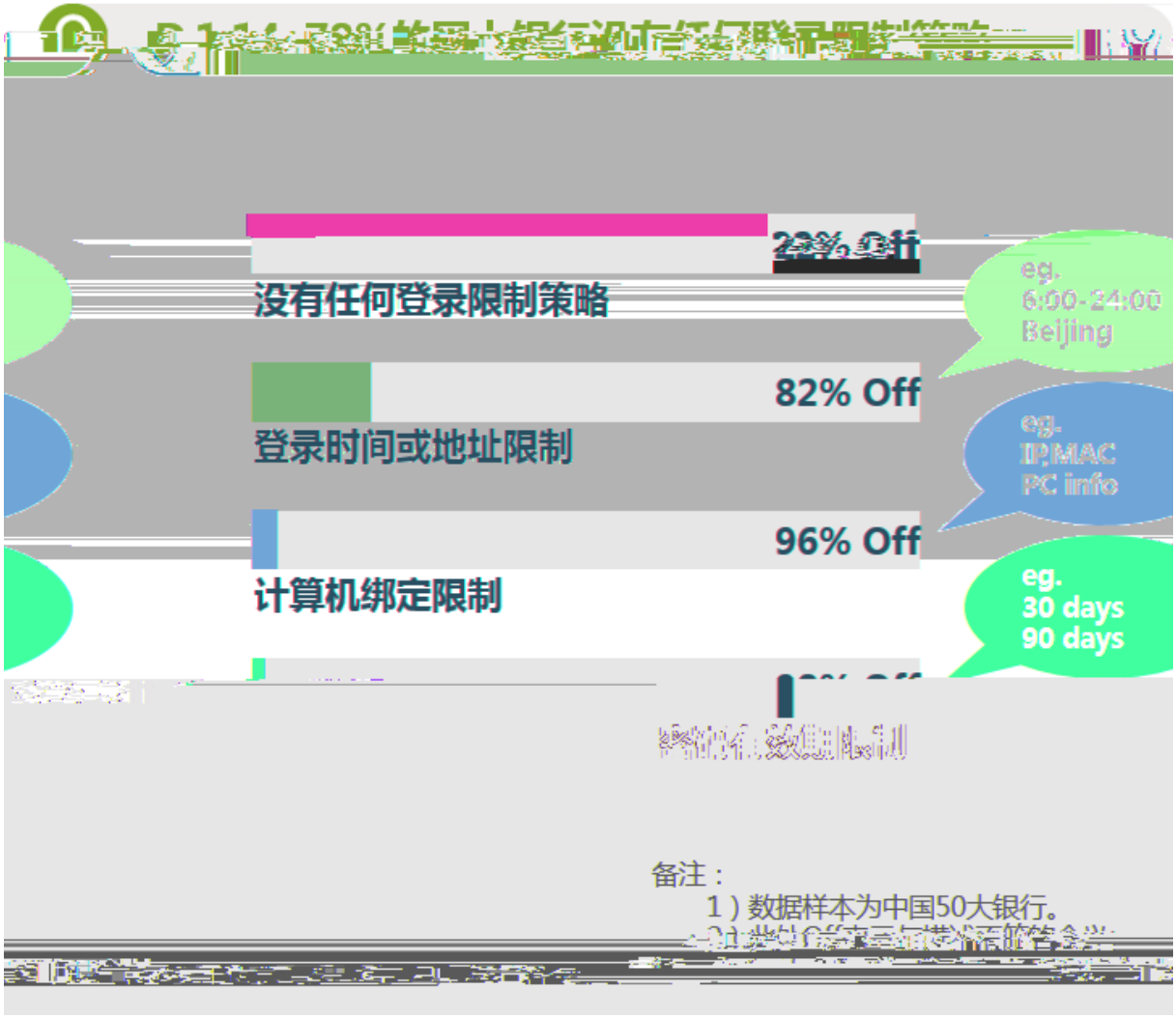
IP ” “ ”

“ 11

” “

”

D.1.14


没有任何登录限制策略
eg.
6:00-24:00
Beijing
82% Off
登录时间或地址限制
eg.
IP,MAC
PC info
96% Off
计算机绑定限制
eg.
30 days
90 days
备注：
1）数据样本为中国50大银行。

D2.

11)

Windows API HOOK

61%

D.2.2

安全控件能够防御

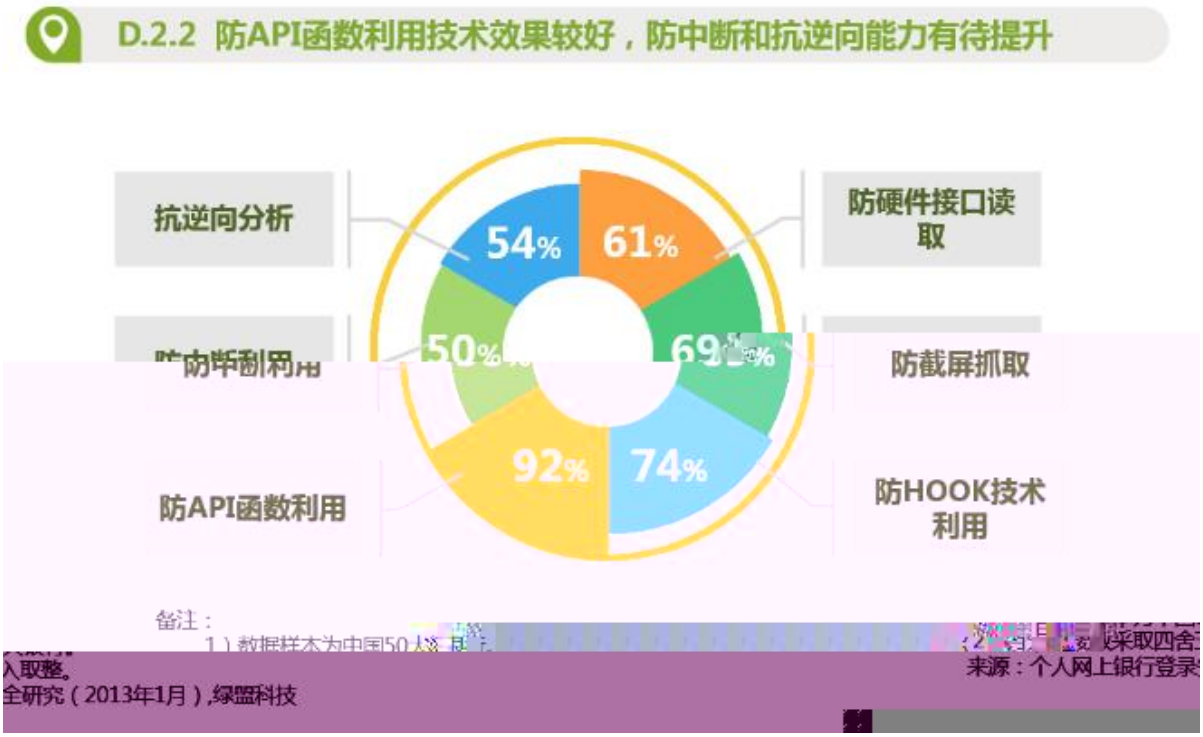
常见的

恶意代码截获

Windows

攻击

API

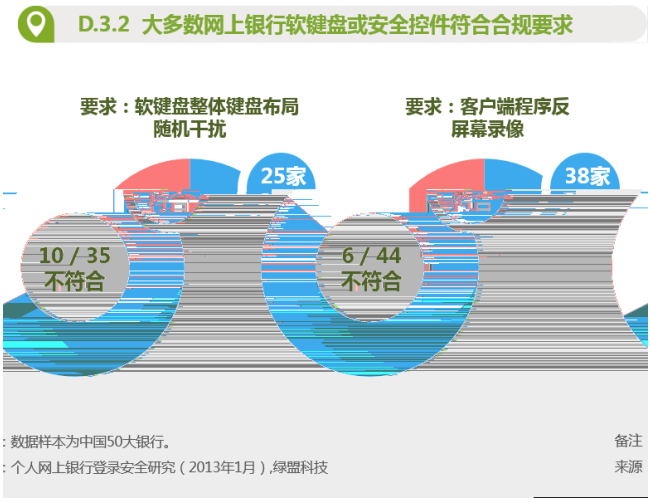


16)

“D1. ” D.1.7

8%

D.3.2



Windows

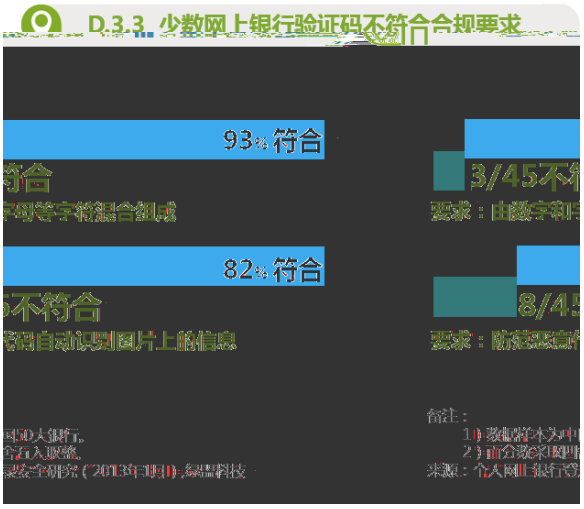
“

100%

”

17)

Token



OCR

D.3.3

45

URL

“

IP

”

18) USBKEY

USBKEY

USBKEY

USBKEY

USBKEY

1) USBKEY

PIN

PIN USBKEY

USBKEY

PIN

2) USBKEY

USBKEY

USBKEY

3)

USBKEY USBKEY

ROM

USBKEY

USBKEY USBKEY

4) USBKEY CPU

USBKEY

USBKEY

1) USBKEY PIN

USBKEY PIN USBKEY

PIN

USBKEY

PIN USBKEY

USBKEY

USBKEY PIN

USBKEY

USBKEY

USBKEY PIN

2) USBKEY “ ”

“ ”

USBKEY

COS Card Operating System

COS

KEY

3)

CA

CA

PKI

4) USBKEY CPU

USBKEY

USBKEY CPU

“ ‘ ’ USBKEY USBKEY

USBKEY

”

4 3
100089
010-68438880
010-68437328
Email market@nsfocus.com

http://www.nsfocus.com/

,
,

巨人背后的专家

THE EXPERT BEHIND GIANTS