



black hat[®]
USA 2018
AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

Are You Trading Stocks Securely? Exposing Security Flaws in Trading Technologies

Alejandro Hernández ([@nitr0usmx](https://twitter.com/nitr0usmx))
Sr. Consultant

 #BHUSA / @BLACKHATEVENTS

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

- From Chiapas, Mexico:



- Consulting and research for IOActive (+6 years).
- No financial background. Initially self-taught in trading.

- Introduction
- Trading software
- Vulnerabilities in Desktop/Mobile/Web platforms
- Responsible disclosure
- Regulators and rating organizations
- Further research
 - Social trading risks
 - Trading protocols
- Recommendations
- Conclusions

- Most of the testing was performed using **paper money (demo accounts)** provided online by the brokerage houses. Only a few accounts were funded with real money for testing purposes. In the case of commercial platforms, the free trials provided by the brokers were used.
- **Only end-user applications and their direct servers** were analyzed. Other **backend protocols and related technologies** used in exchanges and financial institutions **were not tested**.
- This research is **NOT** about High Frequency Trading (**HFT**), **blockchain**, or **how to get rich overnight**.









NYSE

NYSE

GTS

NYSE

USAS

NYSE

PIP

NEW YORK STOCK EXCHANGE

#CNBC

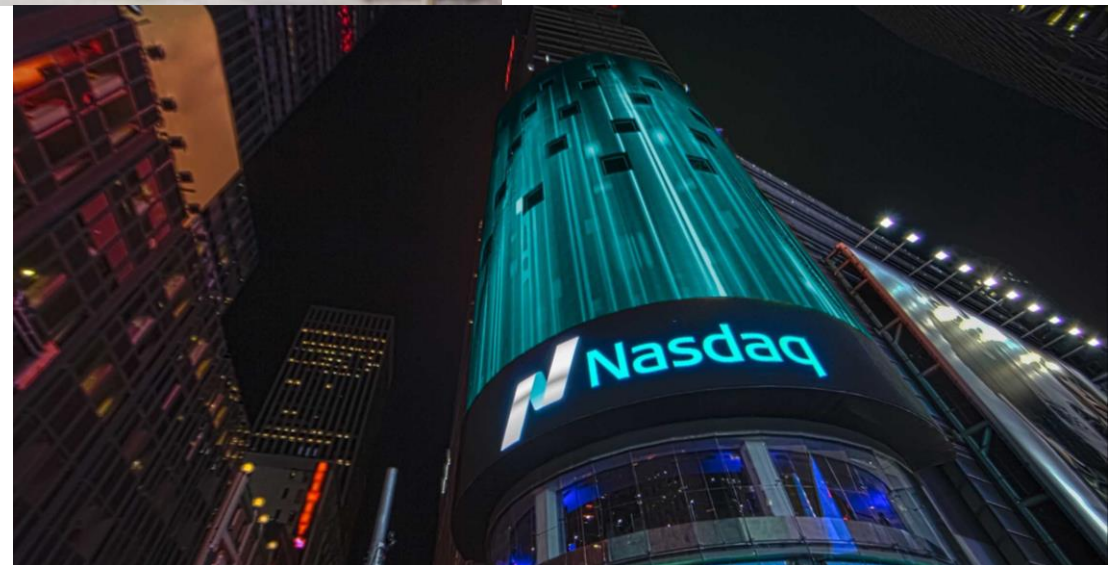
NYSE

NYSE

- Open outcry is gone
- Electronic trading
 - Faster
 - Easier
 - Cheaper



- Stock exchanges
 - NYSE
 - NASDAQ
 - TSE
 - LSE
 - SSE
 - BMV
 - Etc.



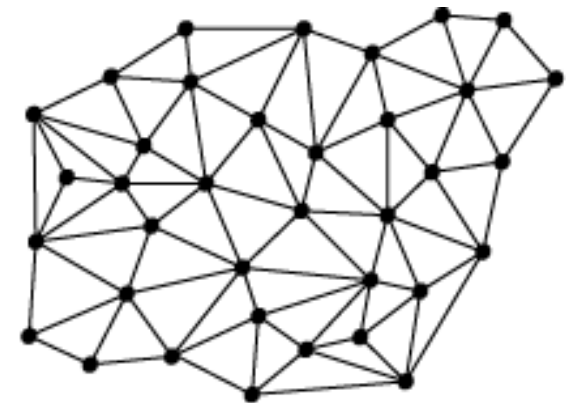
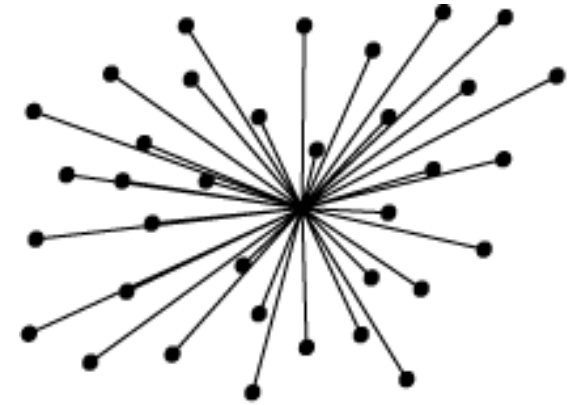
- Public companies
 - Listed in stock exchanges
 - Symbols
 - AAPL
 - NFLX
 - AMZN
 - V
 - OKTA
 - H
 - RACE
 - HACK (Cybersecurity ETF)
 - CIBR (Cybersecurity ETF)
 - Etc.



- Financial instruments
 - Secondary market
 - Stocks
 - Exchange-Traded Funds (ETF)
 - Derivatives market
 - Options
 - Contracts for Difference (CFD)
 - Forex market
 - Currencies
 - Cryptocurrency market



- Banking
 - Centralized in a financial entity
 - One point of failure
- Exchange markets
 - Distributed
 - Records of who owns what, who sold/bought what, and to whom, are not stored in a single place, but many



The **valuable information** as well as the **attack surface and vectors** in trading environments **are slightly different** than those in banking systems.

- Brokerage firms
 - Trading platforms
 - Fund via bank transfers or credit card
 - Monitor cash balances, net worth, margin balance, buying power
 - Monitor your positions (securities you own) and their performance
 - Market research
 - Send buy/sell orders
 - Create alerts/triggers
 - Real-time news and video broadcasts
 - Social trading



Whether you're a speculator, a very active intra-day trader, or simply a buy-and-hold trader, **sensitive data** from the previous list **must be kept secret** and only known by its owner.

- Users per platform
 - **TD Ameritrade:** 11,100,000 funded accounts
 - **Charles Schwab:** 10,755,000 active accounts
 - **MetaTrader:** probably the most used one
 - For Android: +6,000,000 installs
 - **Yahoo! Finance:** 75,000,000 monthly active users
 - **Robinhood:** 3,000,000
 - For Android: +1,000,000 installs



Ameritrade

charles
SCHWAB



MetaTrader

YAHOO!
FINANCE

 robinhood

Sources:

<https://www.amtd.com/investor-relations/by-the-numbers/default.aspx>

<https://www.sec.gov/Archives/edgar/data/316709/000031670918000009/schw-12312017x10k.htm>

<https://techcrunch.com/2017/09/26/investors-can-now-make-trades-on-yahoo-finance/>

<https://www.bloomberg.com/news/features/2018-02-08/brokerage-app-robinhood-thinks-bitcoin-belongs-in-your-retirement-plan>

- Users per platform
 - **Coinbase:** 13,300,000
 - For Android +5,000,000 installs
 - **Markets.com:** 5,000,000
 - **Bloomberg Terminal:** 325,000
 - For Android: +500,000 installs
 - **IQOption:** 25,580,000
 - **AvaTrade:** 200,000
 - **Plus500**
 - For Android: +5,000,000 installs

Sources:

<https://www.cnbc.com/2017/11/27/bitcoin-exchange-coinbase-has-more-users-than-stock-brokerage-schwab.html>

<https://www.markets.com>

<https://www.nytimes.com/2015/04/18/business/dealbook/bloomberg-terminals-outage.html>

coinbase



Bloomberg



iq option

Ultimate trading experience



Plus500

- Users per platform
 - **Money.Net:** 83,000
 - **ExpertOption**
 - For Android: +1,000,000 installs
 - **NinjaTrader:** 40,000
 - **OANDA fxTrade**
 - For Android: +100,000 installs
 - **Thomson Reuters Eikon:** 190,000



Sources:

<https://nypost.com/2017/11/30/money-net-now-has-more-than-80000-paying-customers/>

<https://ninjatrade.com/AboutUs>

<https://www.wallstreetprep.com/knowledge/bloomberg-vs-capital-iq-vs-factset-vs-thomson-reuters-eikon/>

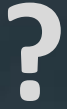








Balances	
All Accounts	
Edit	
ACCOUNT SUMMARY	
Available Funds For Trading:	
Cash & Sweep Vehicle:	
Cash Balance:	
Day Trading Buying Power:	
Equity Percentage:	
Long Marginable Value:	
Long Stock Value:	
Maintenance Requirement:	
Margin Balance:	
Margin Equity:	
Money Market Balance:	
Net Liquidating Value:	
Option Buying Power:	
Short Balance:	
Short Marginable Value:	



TELCEL 12:45 a. m. 79%

Positions

Symbol	P/L Day	P/L Open	P/L
P/L Day:			
P/L Open:			
Net Liq:			
Available \$:			
Equity:			

Quotes Positions Orders Alerts More

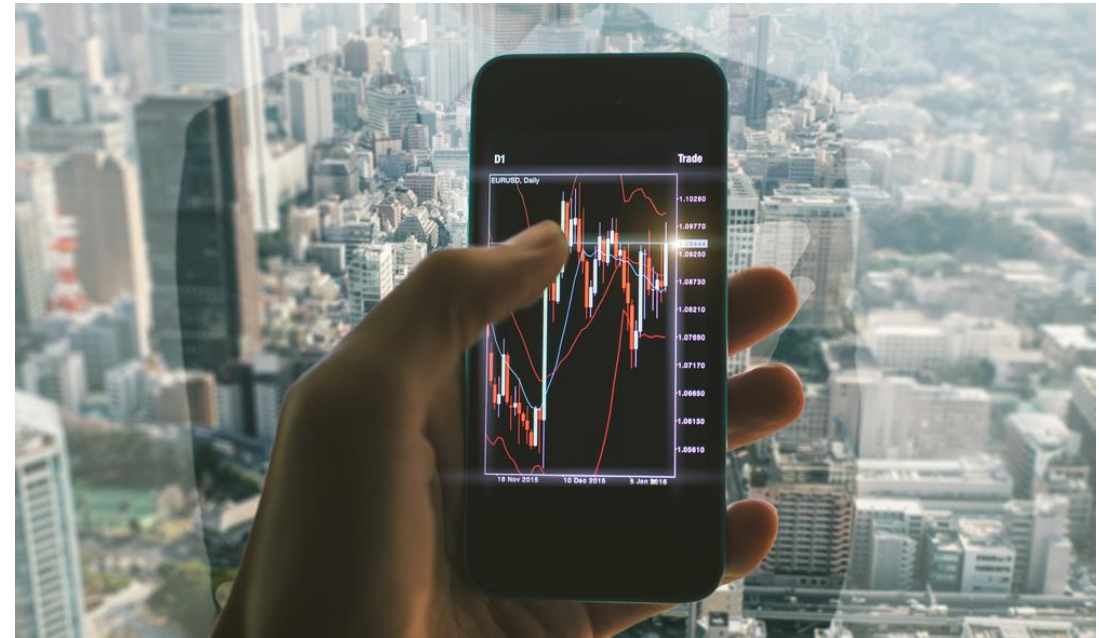
- Scope
 - Some of the **most used and well-known**. Some support cryptocurrency trading.
 - 16 Desktop applications
 - 34 Mobile apps
 - 30 Websites



- Brokers

- Ally Financial
- AvaTrade
- Binance
- Bitfinex
- Bitso
- Bittrex
- Bloomberg
- Capital One
- Charles Schwab
- Coinbase
- easyMarkets
- eSignal
- ETNA
- eToro
- E-TRADE
- ETX Capital
- ExpertOption
- Fidelity
- Firsttrade
- FxPro
- GBMhomebroker
- Grupo BMV
- IC Markets
- Interactive Brokers
- IQ Option
- Kraken
- Markets.com
- Merrill Edge
- MetaTrader
- Money.Net
- NinjaTrader
- OANDA
- Personal Capital
- Plus500
- Poloniex
- Robinhood
- Scottrade
- TD Ameritrade
- TradeStation
- Yahoo! Finance

- Analysis
 - Devices
 - **Windows 7** (64-bit)
 - **Windows 10** Home Single (64-bit)
 - **iOS 10.3.3** (iPhone 6) [not jailbroken]
 - **iOS 10.4** (iPhone 6) [not jailbroken]
 - **Android 7.1.1** (Emulator) [rooted]



- Controls/features reviewed
 - **Just the tip of the iceberg**

Desktop
Two-factor authentication
Automatic logout/lockout for idle sessions
Encrypted communication
Privacy mode
Sensitive data in log files
Secure data storage
Software vulnerabilities
Hardcoded secrets in the application
Anti-exploitation mitigations
Anti-reverse engineering

Mobile
Biometric authentication
Automatic logout/lockout for idle sessions
Privacy mode
Encrypted communication
SSL certificate validation
Session management
Client-side data validation
Sensitive data in logging console
Secure data storage
Root detection
App obfuscation
Hardcoded secrets in code

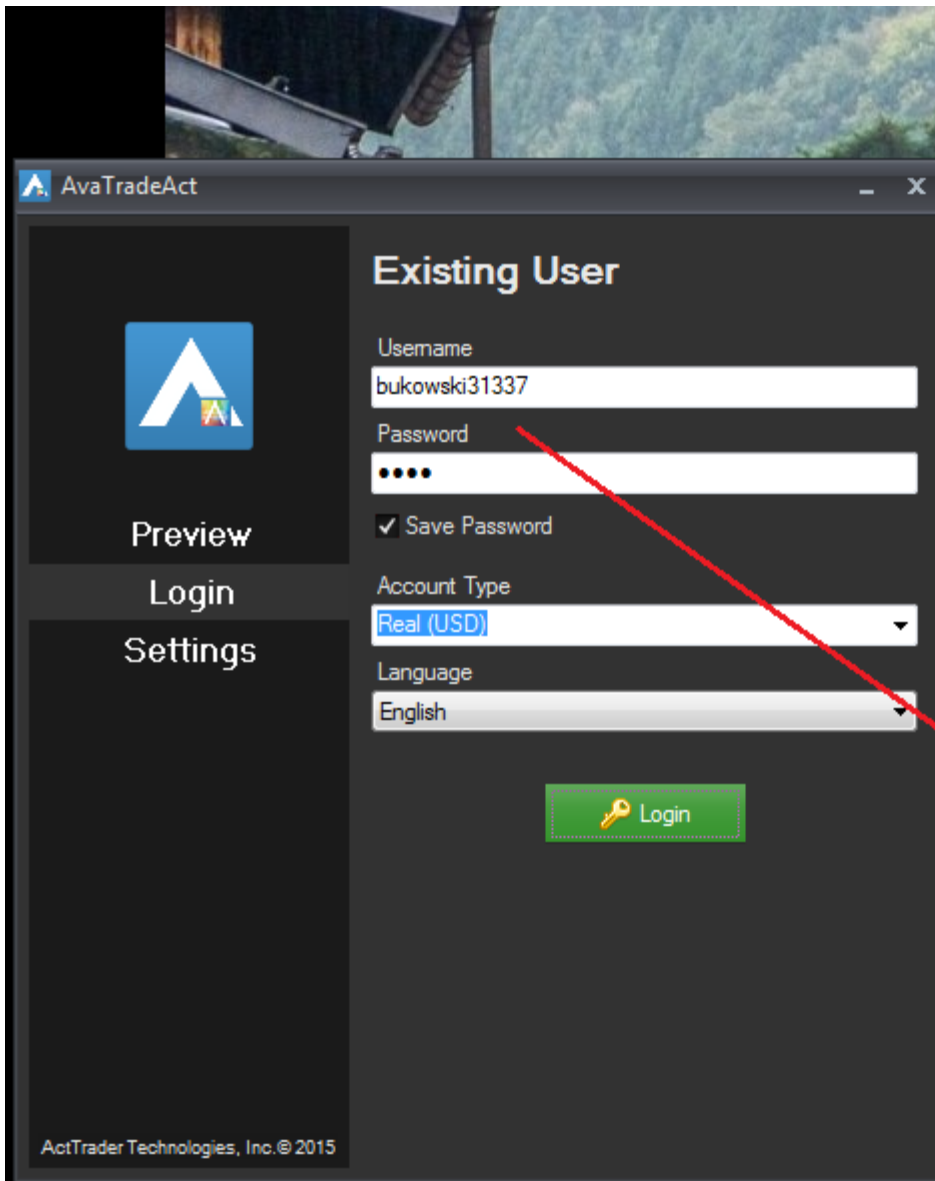
Web
Two-factor authentication
Weak password policy
Encrypted communication
Automatic logout/lockout for idle sessions
Security attributes in session cookies
Session valid after logout
Sensitive data in URL
Insecure site redirect
Cross-site Scripting (XSS) [GET]
Cross-site Request Forgery (CSRF) [GET]
Clickjacking
Security headers
Infrastructure vulnerabilities
Cybersecurity guidance

Unfortunately, the results proved to be **much worse compared with applications in retail banking**. For example, mobile apps for trading are less secure than the personal banking apps reviewed in [2013](#) and [2015](#).

- Medium- to high-risk **vulnerabilities** include
 - Full/partial **encryption** problems
 - Communications
 - Passwords
 - Trading data
 - Denial of Service
 - Authentication
 - Session management
 - Others...



- **Partial/full unencrypted communications**
 - 9 desktop applications (64%)
 - 2 mobile apps (6%)
- Attackers could intercept and alter data, including
 - Bid/ask prices
 - Buy/sell securities based on misleading information
- Most encrypt all the data but a few requests are unencrypted
 - HTTP
 - FIX
 - Proprietary protocols



```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark_C16FE63F-107A-42A7-97CA-3B86177BDE0F_20180610205050_a01908.pcapng

GET /xml/logon?lang=en_US&secure=p&schema%24=eforex35 HTTP/1.1
Timestamp: 2018-06-10 21:50:57.001
X-Auth-SHA1: 3A2799F071009366FAACA4FC91F2E8561A3739AC
Host: real6.sysfx.com:8035
Accept-Encoding: deflate, gzip, identity
User-Agent: FOREST 4.7.223.208/4.7.223

HTTP/1.1 401 Unauthorized
Date: Mon, 11 Jun 2018 01:50:57 GMT
Server: AWS (Ada Web Server) v3.2.0w
WWW-Authenticate: Digest qop="auth", realm="Trade station", stale="FALSE",
nonce="gdUdrCw66bd6f480556af491f8cfcfe8c5719eae"
Connection: keep-alive
Content-Type: text/html
Content-Length: 55

<?xml version="1.0" encoding="utf-8" ?><authorization/>GET /xml/logon?lang=en_US&secure=p&schema%24=eforex35
Timestamp: 2018-06-10 21:50:57.001
X-Auth-SHA1: 3A2799F071009366FAACA4FC91F2E8561A3739AC
Host: real6.sysfx.com:8035
Accept-Encoding: deflate, gzip, identity
User-Agent: FOREST 4.7.223.208/4.7.223
Authorization: Digest username="bukowski31337", realm="Trade station",
nonce="gdUdrCw66bd6f480556af491f8cfcfe8c5719eae", algorithm="MD5", uri="/xml/logon?lang=en_US&secure=p&schem
%24=eforex35", qop="auth", nc=00000002, cnonce="53aae9055ee2a56e5eb0197f685eb154",
response="b0419de066545f777c0977b5d081c874"

HTTP/1.1 200 OK
Date: Mon, 11 Jun 2018 01:50:58 GMT
Server: AWS (Ada Web Server) v3.2.0w
Connection: keep-alive
Content-Type: text/html
Content-Length: 242

<?xml version="1.0" ?>
<error code="20127" message="Wrong Account Type or Username or Password"


```


[USD] AvaTradeAct [PREVIEW]

Home View Trade Windows Charts ActFX FXApps Help

Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_C16FE63F-107A-42A7-97CA-3B86177BDE0F_20180611103504_a08328.pcapng

You will be Buying USD / Selling JPY

Instrument	USDJPY
Account(s)	855985
Amount	3,000
Rate	109.931
Trader Range	0.0

```
GET /xml/create_order?
account=855985&pair_id=3&amount=3000&sb=B&rate=109.931&rate_dt=20180611103531&trader_range=0&w=0&tag=YNAaenHo*4&schema
%24=edforex35&session%24=YNAaenHo HTTP/1.1
Connection: close
Timestamp: 2018-06-11 11:35:34.061
X-Auth-SHA1: B338E82A0A5729928CD15412DC46215DE24802A8
Host: demo6.sysfx.com:13035
Accept-Encoding: deflate, gzip, identity
User-Agent: FOREST 4.7.223.220/4.7.223

HTTP/1.1 200 OK
Date: Mon, 11 Jun 2018 15:35:35 GMT
Server: AWS (Ada Web Server) v3.2.0w
Connection: close
Content-Type: text/html
Content-Length: 468

<?xml version="1.0" ?>
```

Main Dashboard Charts Ins

Dealing Rates Table

Instrument	Sell
EURUSD	1.17943
GBPUSD	1.34099
USDJPY	109.674
USDCHF	0.98530
EURGBP	0.87940
EURJPY	129.357

Archivo Editor Ver Historial Marcadores Herramientas Ayuda

Autochartist

ker=24&v=2.7.81&sid=773C2EE3A3D9D1FB786A5B5

actforex [Logout] English

America/Sao_Paulo

autochartist.com™

Demo Account. Results are delayed.

Our Favourites Trading Opportunities Volatility Analysis Event Impact Analysis Performance Statistics Messaging & Alerts Trading Community

```

Wireshark · Follow TCP Stream (tcp.stream eq 11) · wireshark_C16FE63F-107A-42A7-97CA-3B86177BDE0F_20180610220626_a07324.pcapng

GET /aclite/ACTFOREXMLAPI?
sourceapp=ACTFOREX&locale=en_US&logintoken=E935883B12DF23F33EE9457F0D4C12FF14979AEB14AF8FE7&request=chartpatterns&symbol]=EURUSD
%2CGBPUSD%2CUSDJPY%2CUSDCHF%2CEURGBP%2CEURJPY HTTP/1.1
Timestamp: 2018-06-10 23:10:19.353
X-Auth-SHA1: 3312CA56369A723FBDA48990588FE06A2EE5C045
Host: actforex.autochartist.com
Accept-Encoding: deflate, gzip, identity
User-Agent: FOREST 4.7.223.220/4.7.223

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6FCD971F118C85EDB738D1C561A78B63; Path=/aclite/; HttpOnly
Set-Cookie: rememberMe=deleteMe; Path=/aclite; Max-Age=0; Expires=Sun, 10-Jun-2018 03:09:50 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Date: Mon, 11 Jun 2018 03:09:49 GMT

<Authentication> <sessionid>6FCD971F118C85EDB738D1C561A78B63</sessionid> <errorMessage></
errorMessage> <shortErrorMessage></shortErrorMessage> <mt4timezoneoffset>1000</mt4timezoneoffset>
<webapploginurl>http://actforex.autochartist.com/aclite/DirectMain?apilogintoken=qodfkOyoMac9MSA50trqs004m4COVkJz&rm=1</
webapploginurl> </Authentication>

```

Predef.Stop	Predef.Limit	Time
		09/0
		09/0
		09/0

time	Opened By	Trade ID
2018...		51050877
2018...		51050879
2018...		51050881
2018...		51050883

Wireshark · Follow TCP Stream (tcp.stream eq 9) · wireshark_C16FE63F-107A-42A7-97CA-3B86177BDE0F_20180320184253_a0...

```
DBCQSHdr0300.....Winros 465 11/18/15
Buil.....Z.....bukowski31337.....Qwertyf00b4r.....
.....172.20.5.92.....N.....DC3AD275 78-84-3C-AF-20-
BA.....This protocol and message Copyright 1999 Data Broadcasting Corporation. All
rights
reserved.....
...c..wDBCQSHdr0300.....Winros 465 11/18/15
Buil.....Z.....bukowski31337.....Qwertyf00b4r.....
.....172.20.5.92.....N.....DC3AD275 78-84-3C-AF-20-
BA.....This protocol and message Copyright 1999 Data Broadcasting Corporation. All
rights
reserved...
...c..w
```

eSignal Data Manager
File Data Options Help

**I-Net:Primary Socket no
eSignal Data Manager
NewsServer: Shutdown**

Reception Password Available Memory
NODATA NONE 4294967295 Ld->27%

3 client pkt(s), 2 serv...
Entire conversati...
Find:

Connectivity

- eSignal CM IP Address
- Enterprise Server IP Address
- NewsServer IP Address
- Failover Admin Server Version
- Proxy Static
- Username
- Password

The Merger has been accounted for as a reverse acquisition. Accordingly, the historical financial statements of FT Interactive Data Corporation are the historical financial statements of the Company.

On June 15, 2001, after stockholder approval, the Company changed its name from Data Broadcasting Corporation to Interactive Data Corporation. In connection with its name change, the Company changed its trading symbol from DBCC to IDCO. The Company's common stock is traded on The NASDAQ National Market and began trading under the IDCO trading symbol on June 20, 2001.

In addition, in 2001 the Company... approximately \$43.2 million and in... Merrill Lynch, Pierce, Fenner & S... Analysis of Financial Condition an...

Overview

The Company operates in two

- (1) Institutional services
- (2) Retail Investor services

In the Institutional services segment, we provide action and descriptive information to institutional brokerage firms, insurance companies and other providers of fixed income portfolio assets.

eSignal

"2001 has been a profitable year for our business despite difficult economic conditions and the effects of the market on our customer base.

Throughout the year, we've greatly enhanced the eSignal product line with continuous upgrades

and the addition of institutional products to the marketplace. By leveraging strengths within Interactive Data Corporation, we have

interactive client communications tool, an updated portfolio manager, and the addition of Reuters U.S. Company News to eSignal's online news package.

eSignal Pro™

As a result of several years of infrastructure development and implementation efforts, eSignal introduced a professional version delivered via an ASP

(Application Service Provider) model to

*Conexión de red inalámbr...

File Edit View Go Cap...

tcp.stream eq 25

No.	Time
8743	92.904226
8753	93.048884
8754	93.048922
8755	93.049151
8790	93.420939
8791	93.421007
8797	93.564814
8799	93.611022
8805	93.759187
8806	93.759446

▶ Frame 8791: 457 bytes

▶ Ethernet II, Src: Hor

▶ Internet Protocol Ver

▶ Transmission Control

▶ [2 Reassembled TCP Se

0000	00 50 e8 03 36 67
0010	01 bb 7b 05 40 00
0020	e1 c8 56 89 0f a1
0030	ff f0 be 0b 00 00
0040	69 6f 6e 3d 27 31
0050	6e 67 3d 27 75 74
0060	74 68 6f 64 43 61
0070	6f 64 4e 61 6d 65
0080	65 42 69 74 73 3c
0090	65 3e 0a 20 3c 70
00a0	70 61 72 61 6d 3e
00b0	3e 0a 20 20 20 20
00c0	6b 6f 77 73 6b 69
00d0	69 6e 67 3e 0a 20
00e0	0a 20 20 3c 2f 70
00f0	61 72 61 6d 3e 0a
0100	0a 20 20 20 20 3c
0110	61 37 33 37 35 38

Wireshark · Follow TCP Stream (tcp.stream eq 25) · wireshark_C16FE63F-107A-42A7-97CA-3B861778DE0F_20180320181944_a05...

POST / HTTP/1.1
Content-Type: text/xml
Host: cmfs.esignal.com:4001
POST: /
User-Agent: QxtXmlRpc
Content-Length: 403
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: es-MX,en,*

```
<?xml version='1.0' encoding='utf-8'?>
<methodCall>
  <methodName>GetServiceBits</methodName>
  <params>
    <param>
      <value>
        <string>bukowski31337</string>
      </value>
    </param>
    <param>
      <value>
        <string>3c6a7375875779a794daf0d0d6c8e4df</string>
      </value>
    </param>
    <param>
      <value>
        <string>750cbb53605036582c48e905ccabac58</string>
      </value>
    </param>
  </params>
</methodCall>
HTTP/1.1 200 OK
Server: XMLRPC++ 0.7
Content-Type: text/xml
Content-length: 165

<?xml version="1.0"?>
<methodResponse><params><param>
  <value><array><data><value>USERNOTFOUND</value></data></array></value>
</param></params></methodResponse>
```

eSignal

eSignal cannot establish a connection due to internet connectivity issues or an invalid username/password.


User Name: bukowski31337

Password:

[Forgot your password?](#)

Login Automatically

OK Cancel



- **Partial/full unencrypted communications**
 - **FIX:** Financial Information eXchange Protocol
 - Initiated in 1992
 - Industry standard for messaging and trading
 - Widely used by exchanges and traders
 - Guidelines on how to implement it through a secure channel

Example of a FIX message : Execution Report (Pipe character is used to represent SOH character)

```
8=FIX.4.2 | 9=178 | 35=8 | 49=PHLX | 56=PERS | 52=20071123-05:30:00.000 | 11=ATOMNOCCC9990900 | 20=3 | 150=E | 39=E | 55=MSFT | 167=CS  
| 54=1 | 38=15 | 40=2 | 44=15 | 58=PHLX EQUITY TESTING | 59=0 | 47=C | 32=0 | 31=0 | 151=15 | 14=0 | 6=0 | 10=128 |
```

FIX



FIX TRADING COMMUNITY™
INDUSTRY-DRIVEN • INDEPENDENT • NEUTRAL



Account

- Properties
- Password
- Email Alerts

Application

- General
- Assets
- Market Watch
- Notifications
- QuickTrade
- Hotkeys

Advanced

- Email
- Connection
- FIX API**

FIX API

You can find specifications and code samples here - [FIX API help](#)

Price Connection

Copy to Clipboard

Host name: h1.p.ctrader.cn
 (Current IP address 119.81.178.126 can be changed without notice)
 Port: 5211 (SSL), 5201 (Plain text)
 Password: ***** (a/c 10180548 password)
 SenderCompID: fxpro.10180548
 TargetCompID: cServer
 SenderSubID: QUOTE

Trade Connection

Copy to Clipboard

Host name: h1.p.ctrader.cn
 (Current IP address 119.81.178.126 can be changed without notice)
 Port: 5212 (SSL), **5202 (Plain text)**
 Password: ***** (a/c 10180548 password)
 SenderCompID: fxpro.10180548
 TargetCompID: cServer
 SenderSubID: TRADE

Note: cTrader is available in both [Netted](#) and [Hedged](#) accounts. You may want to request a Netted account type from your broker for aggregate position trading

GBPUSD, h1



News

New Order

DEMO



**Interactive Brokers TWS
iBot sending voice commands
unencrypted over FIX
(Financial Information
Exchange Protocol)**



Monitor Portfolio Favorites US Movers Filter ?

P&L + PROFILE Margin + ACCOUNT

DAILY **-1,178** Unrealized 241.7K
 Since prior Close -0.05% Realized -2.1K

Net Liq 2.3M Excess Liq 1.7M
 Maintenance 554.7K SMA 92.4K

POSITIONS	DLY P&L	POS	MKT VAL	LAST	AVG PX
My Investments	-6,245		994,156		
FSLR	-524	1,234	93,167	75.50	75.925
ISRG	-675	1,337	619,365	463.25	463.755
PLNT	-5,047	26,920	1,095,913	40.72	40.821
USD Cash			-814,289		

Login

User name bukow137

Password

Trading Mode Live Trading

Color Palette dark

Use/store settings on server

Use SSL

More options Login Cancel

```

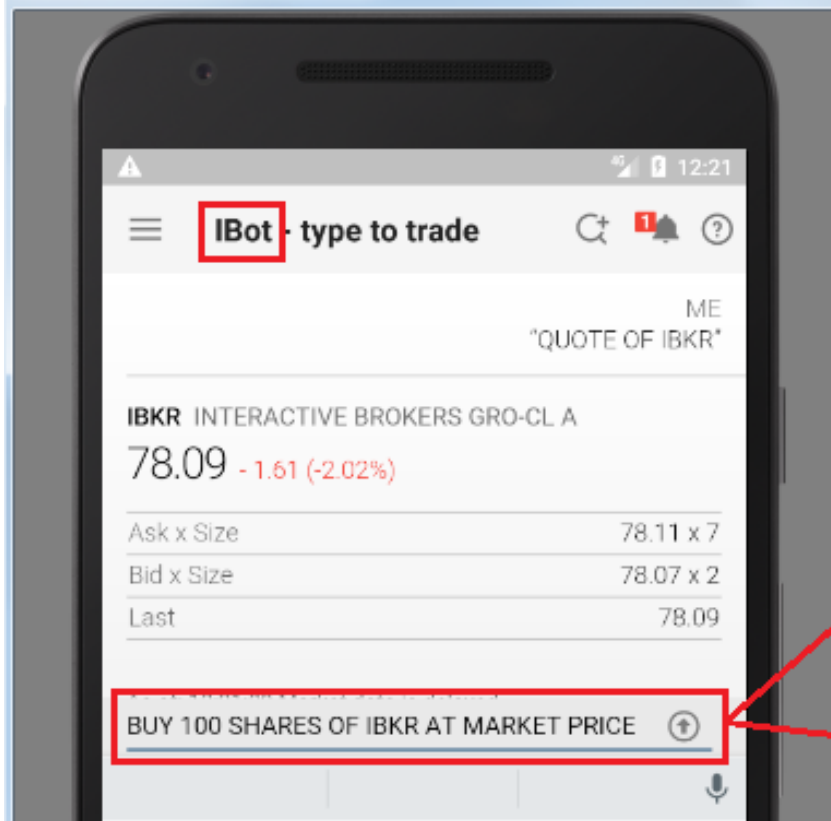
E63F-107A-42A7-97CA-3B86177BDE0F_20180419102249_a03928
...@.3@.....8=0.9=0024.35=G... .0D.@_.....8=0.
...a.@R.....8=0.9=0041.35=G... ..$n.@Q.....0B.@H.E.....8=0.
.]n.0....(.,$......q.Xn.....Q..Bp...^..@.b.`.....
.\.l..$....l.Q..n.....m...R.+..o.....
A*.=D.!g...M.....;D16x.^>.:1.... &.(.....+...p.....c&q..)D`3....
.y.....J.M..[+.4kyv{.l.-o;V..&.....n...]/.]....e.....|.?;.K.....?'/\.8=0.9=0027.35=Q.44714,193,0.01,0,0,9c,8=0.
9=0027.35=Q.44715,194,0.01,0,0,9c,8=0.9=0027.35=Q.44716,195,0.01,0,0,a6,8=0.9=0013.35=G..0.....8=0.
9=0585.35=G.....<.....MTFL...
MTFL$07a9d994.....Z.....L{K:n/a}Intuitive Surgical (ISRG) Q1 2018 Earnings Conference Call Transcript..Ku....MTFL...
MTFL$07aa27f7.....Z...s...C{K:-1.00}International Headwinds Can't Slow Intuitive Surgical Inc....Ku....SA-PRO.....SA-
PRO$07ab0fe3.....Z.....F{K:1.00}Technology Is Pushing Up Stocks - Cramer's Mad Money (4/18/18)....Ku....MKR.....MKR
$07ab21f2.....Z.....I{K:1.00}Intuitive Surgical: S&#038;P 500&#8217;s Top Gainer on April 18 .....Ku....ZK.....ZK
$07abe324.....Z..@...&{K:-1.00}Company News For Apr 19, 2018....Ku8=0.9=0013.35=G..0.....8=0.9=0813.35=G..0.....
.....SS.....SS$07a96497.....Z.a.....{K:1.00}FSLR Positive - $FSLR Monthly. Highest level since 2011 for domestic
solar trying to clear massive base bottom. "The bigger the bas&#x2026; https://t.co/h6RyT4Logp..{.....SS.....SS
$07a9a7d3.....Z.....{K:1.00}FSLR Positive - RT @chessNwine: $FSLR Monthly. Highest level since 2011 for domestic
solar trying to clear massive base bottom. "The bigger the base, the h&#x2026;..{.....MTFL...
MTFL$07ab1c9e.....Z.....T{K:1.00}SunPower Buys Former Nemesis SolarWorld in Play to Expand U.S. Manufacturing.
{.....SS.....SS$07ab6c09.....Z.....d{K:1.00}FSLR Positive - First Solar $FSLR Upgraded to Buy at Bank of America
https://t.co/HWB1mk0U9g.{.....SA-PRO.....SA-PRO$07abe788.....Z.....#{K:n/a}SunPower Dumps Trump Tariffs..{..8=0.
9=0013.35=G..0.....8=0.9=0437.35=G.
p.....ZCK.....ZCK$07873178.....Z.....({R}PLNT: Planet Fitness, Inc. (snapshot).....ZCK.....ZCK
  
```

```

haves China Large Cap", "Buy 100 shares of Chevron", "Buy 100 shares of Walt Disney Company", "Buy 100 shares of Mitsubishi UFJ Financial", "Buy
100 shares of Allergan PLC", "Buy 100 shares of Novartis AG", "Buy 100 shares of Ishares US Real Estate", "Buy 100 shares of Consumer Staples
SPDR", "Buy 100 shares of Home Depot", "Buy 100 shares of UnitedHealth Group", "Buy 100 shares of WalMart Stores", "Buy 100 shares of Internatio
nal Business Machines", "Buy 100 shares of Gilead Sciences", "Buy 100 shares of Boeing Company", "Buy 100 shares of McDonald's", "Buy 100 shares
of Comcast", "Buy 100 shares of Pfizer", "Buy 100 shares of Honeywell International", "Buy 100 shares of Reynolds American", "Buy 100 shares of
Twitter", "Buy 100 shares of China Southern
05-14 12:19:39.955 2904 2921 I aTws : [OUT-0]: 8=FIX.4.1@9=0110@35=JP@320=102@6040=BOT@8082=<"T": "AT", "P":<"CT":<"rasterWidth":384,"ras
terRatio":2.625,"buttonsPerPage":13}>>@10=066@

```

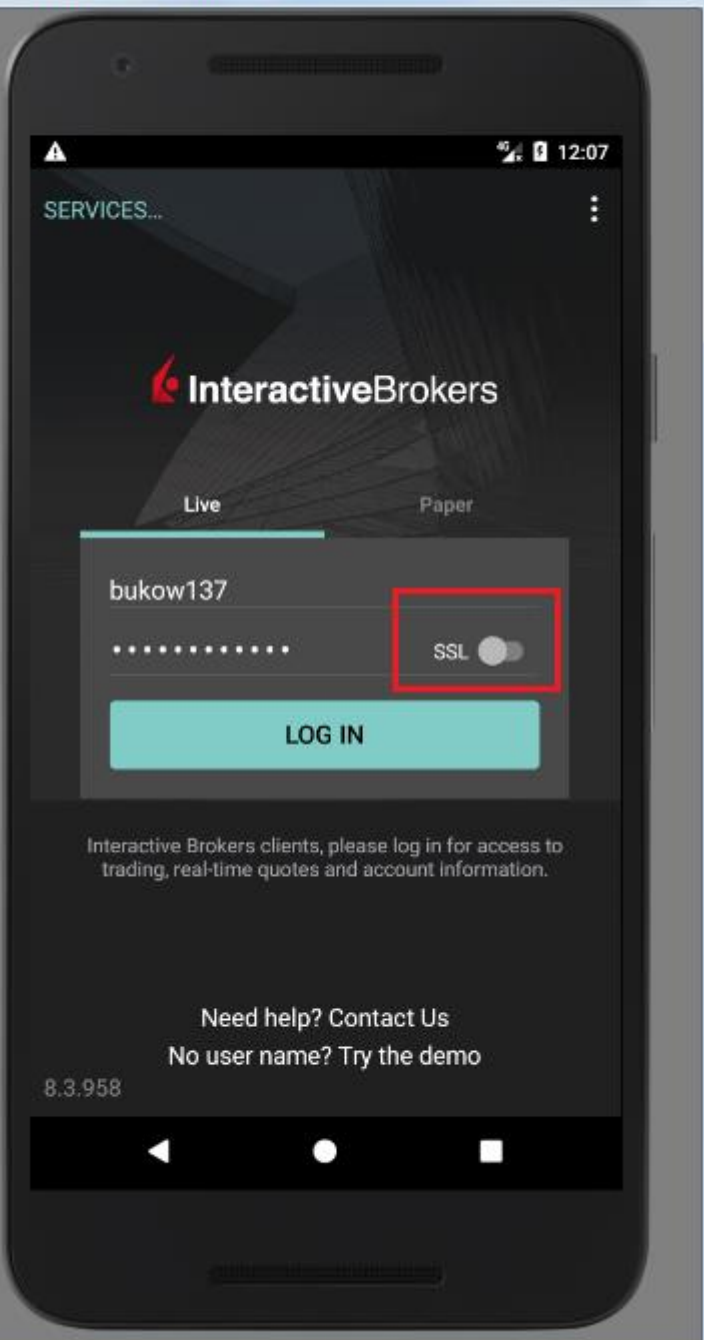
Android Emulator - nexus:5554



```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_4_interfaces_20180514122148_a04844...
8=FIX.4.1.9=0052.35=mt.320=106.8082={"a":"c", "c":"61", "t":"48110.4"}.10=085.8=FIX.
4.1.9=0028.35=mt.320=106.8082={"ok":1}.10=225.8=FIX.4.1.9=0141.35=JP.320=107.6040=BOT.
8082={"T":"IN", "P":{"text": "BUY 100 SHARES OF IBKR AT MARKET PRICE" "device":
{"rasterWidth":256, "buttonsPerPage":5}}}.10=033.8=FIX.4.1.9=0059.35=JP.
320=107.6034=1.6040=BOT.8082={"P":{ }, "T":"IN", "V":1}.10=015.8=FIXCOMP.9=229.x.=.Ak.
0...?1:'A.....cPJ....R
my holdings.">], "BN":1}, "T":"N", "U":1}>@320=13@
-01: processJson: {"P":{"MO":1, "E":{"R":0, "D":1525696441, "MS":"IBKR FYI: Earnings Notificat
portfolio will announce earnings as below<br /> - PLNT declaring Q1 '18 earning on 2018-05-0
M USD. Accounts: D****0182 <br /><br />Please see <a href="https://kb.clientam.com/n
"FN":"Upcoming Earnings", "I":"","ID":"2018050710293516", "HT":0, "FC":"EA", "FD":"Notify me of
oldings.">], "BN":1}, "T":"N", "U":1}
[IN-0-0]: not supported badge for launcher: com.google.android.apps.nexuslauncher
-01: FYI: Received notification:FYINotification [id=2018050710293516, type=FYIPropertyType [
7 07:34:51 CDT 2018, read=false, summary=[IBKR FYI: Earnings Notification], description=[ht
announce earnings as below<br /> - PLNT declaring Q1 '18 earning on 2018-05-08 AfterClose. C
s: D****0182 <br /><br />Please see <a href="https://kb.clientam.com/node/2133">KB2133</a>
-01: 35=u@34=000003@52=20180514-17:21:04@6040=H@320=5431@
-01: 8=FIX.4.1@9=0021@35=u@6040=h@320=5431@10=131@
Bridge]: sendToNativeApp
-01: 8=FIX.4.1@9=0116@35=JP@320=104@6040=BOT@8082=<"T": "IN", "P":<"text": "QUOTE OF IBKR", "devi
251@
-01: <"P":{ }, "T":"IN", "U":1}
-01: 8=FIX.4.1@9=0067@35=mt@320=105@8082=<"a":"c", "c":"61^8^9^4^62^63^64", "t":"48076.5">@10=1
-01: 35=mt@320=105@8082=<"ok":1}>@
-01: 8=FIX.4.1@9=0052@35=mt@320=106@8082=<"a":"c", "c":"61", "t":"48110.4">@10=085@
[JavaBridge]: sendToNativeApp
[OUT-0]: 8=FIX.4.1@9=0141@35=JP@320=107@6040=BOT@8082=<"T": "IN", "P":<"text": "BUY 100 SHARES OF IB
KR AT MARKET PRICE", "device":<"rasterWidth":256, "buttonsPerPage":5}>>@10=033@
-01: 35=mt@320=106@8082=<"ok":1}>@
[IN-0-0]: <"P":{ }, "T":"IN", "U":1}
[IN-0-0]: <"P":{ }, "T":"IN", "U":1}
[OUT-0]: 8=FIX.4.1@9=0067@35=mt@320=108@8082=<"a":"c", "c":"61^8^9^4^62^63^64", "t":"48114.7">@10=1
20@
-01: 35=mt@320=108@8082=<"ok":1}>@
[JavaBridge]: sendToNativeApp
[OUT-0]: 8=FIX.4.1@9=0115@35=JP@320=109@6040=BOT@8082=<"T": "IN", "P":<"text": "SUBMIT ORDER", "devic
e":<"rasterWidth":256, "buttonsPerPage":5}>>@10=228@

```



0x900 imply creation of host color buffer

Update:Allocation Details <
ID=DU1010182+A+T,A];accounts Codes:[DU1010182]

[Account[MGKS Asset Management - All, all
Account[MGKS Asset Management - Core, alloc ID=DUC
0182+A+S,A]=[
Account[All, alloc ID=DU1010182+A+A,A], Account[My
00074+A+S,A]]
MODEL, ALL]]

Update:Allocation Details <
ID=DU1010182+A+T,A];accounts Codes:[DU1010182]

[
0=DUC00074+A+S,A]=[Account[MGKS Asset Management - All, all
+M+S,A], Account[MGKS Asset Management - Core, alloc ID=DUC
0182+A+S,A]=[
+T,A]=[Account[All, alloc ID=DU1010182+A+A,A], Account[My
00074+A+S,A]]
MODEL, ALL]]

0x900 imply creation of host color buffer
0x900 imply creation of host color buffer
0x900 imply creation of host color buffer
6:atws.shared.a.c:20ef654f3
08082=({'a':'c','c':'82^7^8^4^4^84^65^66','t':'50822.6'})@10

5:d.b.a.b\$102e42da7

: [main]: AccountListeners count<add>:6:d.b.a.b\$102e42da7

: [OUT-2]: 8=FIX.4.109=0043035=n0320=37401=DU1010182+A+A@6040=807233=1010=1380

: [IN-2-0]: 3F=n0220=27406040=057119=Balances@7121=Total USD@7100=Net Liquidation Value@7101=2.380.002

tainty@7101=1,343 @7100=Equity with Loan Value@7101=2,378,659 @7100=Previous Day Equity with Loan Value@7101=

s Position Value@7101=3,076,395 @7100=Cash@7101=-695,804 @7100=MTD Interest@7101=-590 @7100=Pending Debit Car

ities USD@7100=Net Liquidation Value@7101=2,380,002 @7100=Equity with Loan Value@7101=2,378,659 @7100=Previou

01=2,404,661 @7100=Securities Gross Position Value@7101=3,076,395 @7100=Cash@7101=-695,804 @7100=MTD Interest

TD Interest@7101=0 @7100=Pending Debit Card Charges@7101=0 @

I Bloomberg: <"BBCL": "AQIAAAAQeZRoUAF2X1ytBbPtHFEBsQAAAAAAAAABAF5yQZ3FFsK9z+JCYQuMPaU6myJA2Uz1+p34wrUWHn+os4b0

xSzJE01A==">

BALANCES		TOTAL USD
Net Liquidation Value	2,380,002	
Net Liquidation Uncertainty	1,343	
Equity with Loan Value	2,378,659	
Previous Day Equity with Loan Value	2,404,661	
Securities Gross Position Value	3,076,395	
Cash	-695,804	
MTD Interest	-590	
Pending Debit Card Charges	0	

tainty@7101=1,343 @7100=Equity with Loan Value@7101=2,378,659 @7100=Previous Day Equity with Loan Value@7101=

s Position Value@7101=3,076,395 @7100=Cash@7101=-695,804 @7100=MTD Interest@7101=-590 @7100=Pending Debit Car

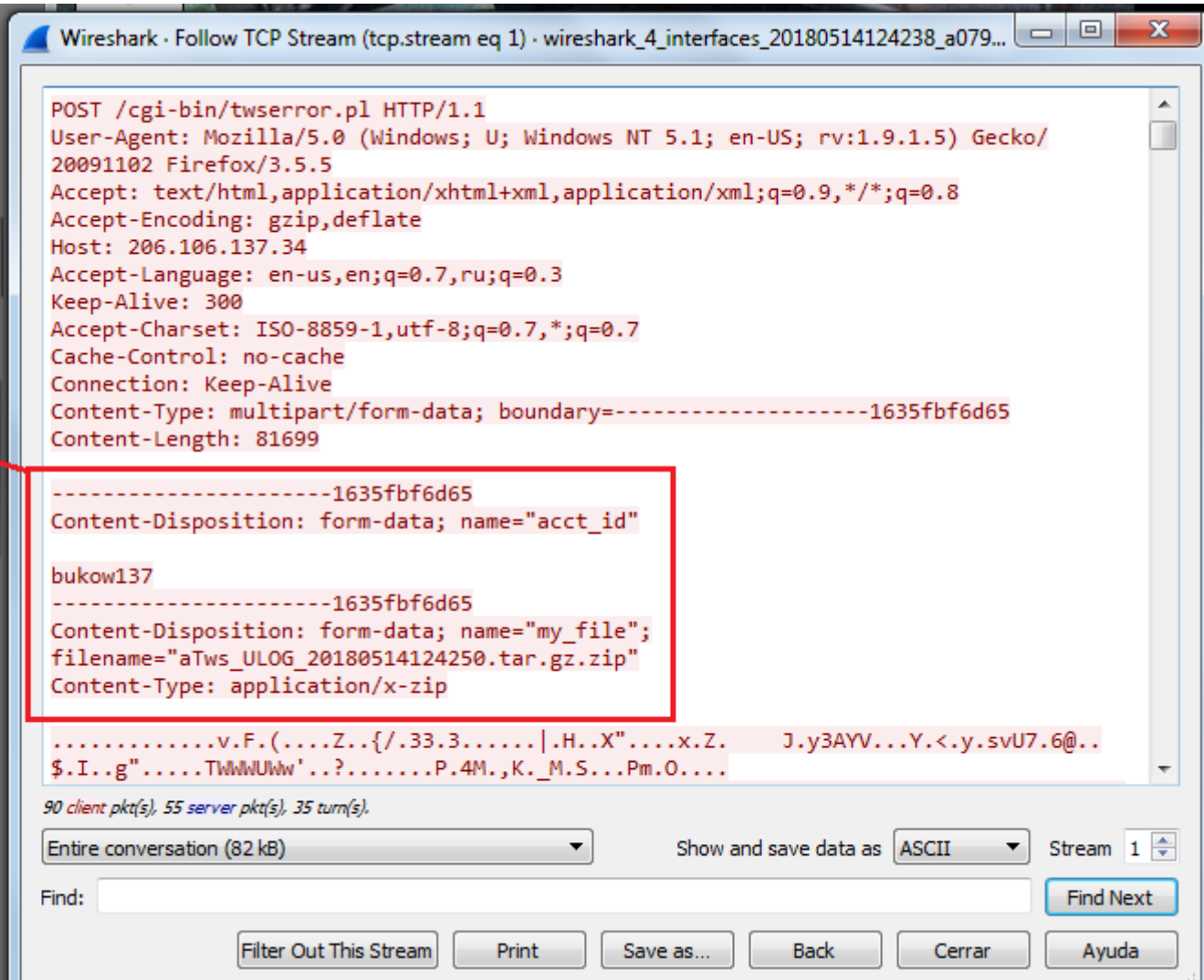
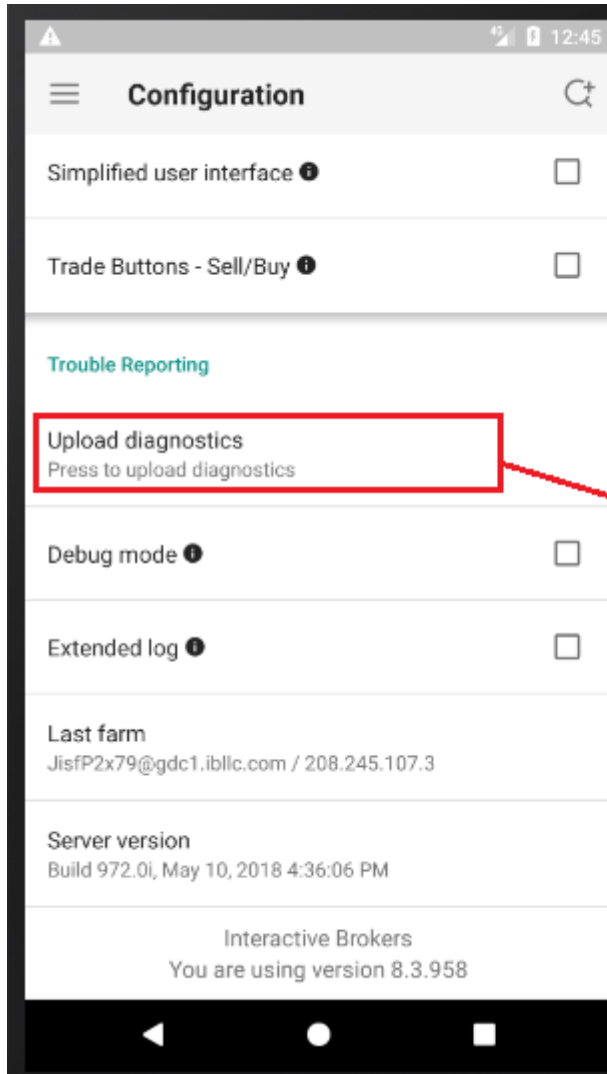
ities USD@7100=Net Liquidation Value@7101=2,380,002 @7100=Equity with Loan Value@7101=2,378,659 @7100=Previou

01=2,404,661 @7100=Securities Gross Position Value@7101=3,076,395 @7100=Cash@7101=-695,804 @7100=MTD Interest

TD Interest@7101=0 @7100=Pending Debit Card Charges@7101=0 @

I Bloomberg: <"BBCL": "AQIAAAAQeZRoUAF2X1ytBbPtHFEBsQAAAAAAAAABAF5yQZ3FFsK9z+JCYQuMPaU6myJA2Uz1+p34wrUWHn+os4b0

xSzJE01A==">



Watch List

My Positions TO INVEST LATER

Add Symbol(s) Add Add Group Sync Off Act

#	Symbol	News	Last Trade	Change	% Change
1	WWE		51.42	+1.11	+2.21
2	PS		21.12	+0.88	+4.40
3	SPOT		151.49	-7.96	-5.01
4	NFLX		324.18	-1.04	-0.32
5	AMX		16.35	-0.03	-0.18
6	HACK		37.29	+0.08	+0.22
7	LOCO		10.85	+0.05	+0.46
8	AAPL		186.53	-0.68	-0.36
9	TSLA		276.81	-7.72	-2.71



Wireshark · Follow TCP Stream (tcp.stream eq 14) · schwab_streetsmart

```

(63.HS.<...F...".m..mB...f{:A.6.1.11
.7.Ya.o.B.....`|x.3. ....K... M
.#.O.:|x.....a:|x.....a2|1|PS|
44Y|1|PS|
G4Z|1|PS|
{"Advise":3001,"Echo":299,"SymbolArray":["PS"]}
14\|1|PS|
R|1|PS
Q|301|PS|180518|0000|190518|1259|1|1
Q|302|PS|180518|0000|180518|1619|1000|1
3^|x.E0aK.0..._Q...$......2.S.u..}(k..j+N?...0....='
....T.6.U..T4...G*j.....{`.. /K_WLXx..*....0...'5..%Xw
n.unW...>,...j.n....Hl...H...m}~..smo...XF"+_;at.D".~;)\
.T.n#...../o.E|x...Qq..
...1.....J|x.3. ....K....?..q#.;D|x...Qq..
...1.....|x.....ak|x.3....q...12.1M.1...H...Og.
.&FF.)@.1`.....10.2|1|SPOT|
44_|1|SPOT|
G4~|1|SPOT|
{"Advise":3001,"Echo":305,"SymbolArray":["SPOT"]}
14b|1|SPOT|
R|1|SPOT
Q|307|SPOT|180518|0000|190518|1259|1|1
Q|308|SPOT|180518|0000|180518|1619|1000|1
5o|x.uQMo.0...WX9..";..4eK.|.$DB ..vE....4..=1....."

```

80 client pkt(s), 474 server pkt(s), 87 turn(s).

Entire conversation (77 kB) Show and s

Find:

Filter Out This Stream Print Save as...

Current build: 1.54.89.0

Hide Balances

Launch Tools Find Active Tools

OKTA Go 50.07 +0.3514 (0.71%) Okta Inc NASDAQ

This account is set to liquidate only. Only existing positions can be reduced or closed.

Bid: 50.07 Ask: 50.10 Volume: 655,780
Open: 50.12 Prev Close: 49.72 Spread: -0.03
High: 50.86 Low: 50.071 Size: 200 X 100

Last Trade	Change	% Change
150.55	-0.25	-0.17
328.87	+4.69	+1.45
16.21	-0.15	
37.27	-0.02	
10.80	-0.05	
187.21	+0.90	
283.30	+6.48	
40.32	+0.38	
43.89	-0.89	

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_C16FE63F-107A...

```
.....F%8 ...0.. .n..o.T...9.....2...a...y.. ....._17|x.  
3..qt...11...u.....1M..I2...A..\F5...P.a  
.....h...o....A....v.....14....Dp2|1|OKTA|  
1@|x.3. ....w.11.s.....C7....g.....eT.....P.....#.....  
3JBq...t....j.C \....a.41g|1|OKTA|  
G1h|1|OKTA|  
e|1|OKTA|  
g1i|1|OKTA|  
8|1|A|OKTA|-1|  
A1j|1|A|OKTA|-1|  
U1k|1|OKTA|  
2|1|OKTA|  
41l|1|OKTA|  
01m|1|OKTA|  
6E|x....R.@...y  
.....L2.d. ..B.&|X.n.%.....'$.....=n.Tg.....  
0&....."#Q.#s`..A..}.|..?..8.....}>.  
|Z.)..E>)...v..(\0...IqT.....6.Z...t;x.vG...;.....x.....
```

CA: Administrador: Símbolo del sistema

```
C:\Users\nitr0us\AppData\Roaming\IQ Option>egren -nir 59db7ec25f4d3ad83fbd8a71cef701ac *  
cfg.dat:1:{"ssid":"59db7ec25f4d3ad83fbd8a71cef701ac","user_id":21519658,"locale":"en","user_locale":"en_US","  
itrousenador@gmail.com","token":"8d74eab5b2137dd8004cd4606c05532081c8940791f3a7efdef031468375f379be68a4b78caa  
7a8182736e0bfc933d62a","tokenHost":"iqoption.com:443","show_lowfps_notice":true,"user_agent":"","device_id":"  
D8257","theme":"blue","theme_plot_bg_visibility":true,"login_plot_mode":"area","login_regulator_logos":false,  
s":"127.0.0.1","proxy_port":"8080","proxy_login":"proxy","proxy_password":"s3cr3t"}
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_C16FE63F-107A-42A7-97CA-3B86177BDE0F_20180402174820_a05520

```
POST //api/v1/events HTTP/1.1  
Host: event.iqoption.com  
Accept: /*/*  
Accept-Encoding: deflate, gzip  
Cookie: uat=c9c64e071d2853bc7906c017a231ad1cc46ab630; lang=en_US; platform=8; platform_version=1017.5.6878.release;  
ssid=59db7ec25f4d3ad83fbd8a71cef701ac; tutorial=;  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.71 Safari/537.3  
Connection: close  
Content-Type: application/json  
X-Action: bulk  
Content-Length: 14617  
  
[{"name":"performance","user_id":21519658,"device_id":"25e82fc1-  
f507-411b-8b5a-32fc5d2704b4","category":"system","platform_id":  
8,"app_version":"1017.5.6878.release","technical_logs":true,"parameters":  
{"candles":"0","cpu":"5.95686","device":"Laptop","disconnects":"0","disconnectsNotification":"0","endpoint":"iqoption.c  
"..."
```


	Connection	Display name	Buying power	Cash value	Excess intrada	Excess initial n	Intraday margir	Initi
●	My NinjaTrader Continuum	Sim101	\$0.00	\$100,000.00	\$100,000.00	\$100,000.00	\$0.00	\$0.0
●	My NinjaTrader Continuum	Account1	\$0.00	\$100,000.00	\$100,000.00	\$100,000.00	\$0.00	\$0.0
●	My NinjaTrader Continuum	Secret Account	\$0.00	\$233,000.00	\$233,000.00	\$233,000.00	\$0.00	\$0.0

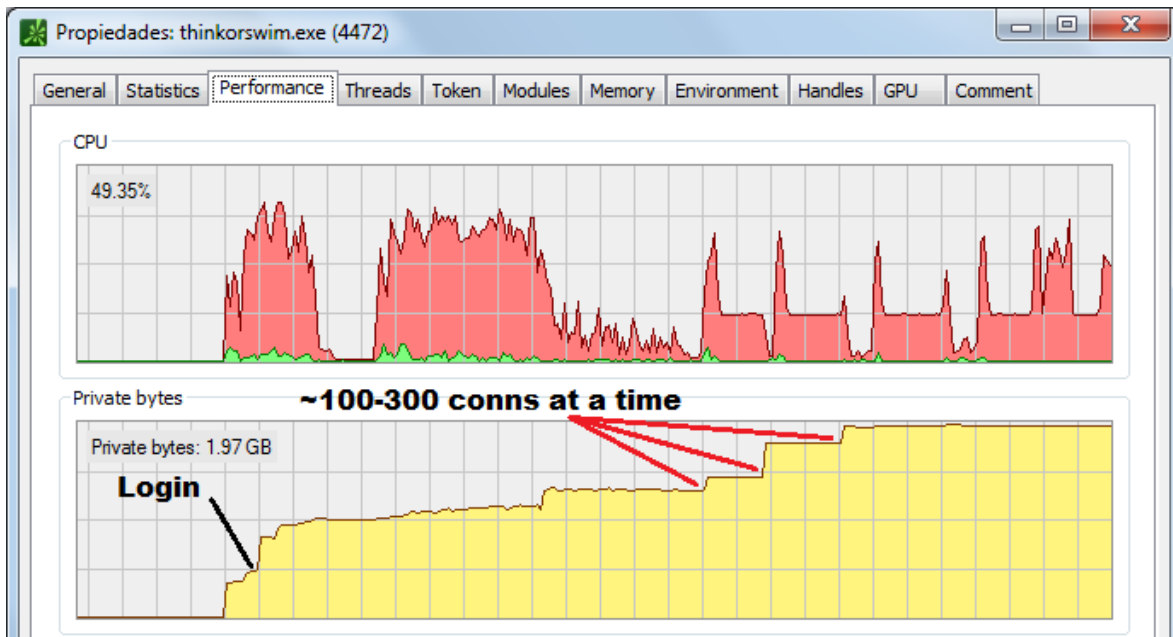
```

nitro0us@bukowski: ~
nitro0us@bukowski:~$ nc 192.168.241.1 36973 -v
Connection to 192.168.241.1 36973 port [tcp/*] succeeded!
2Orders|2Strategies|2BuyingPower|02CashValue|1000002RealizedPnL|02Orders|Sim1012Strategi
es|Sim1012BuyingPower|Sim10102CashValue|Sim1011000002RealizedPnL|Sim10102Orders|Account1
2Strategies|Account12BuyingPower|Account102CashValue|Account11000002RealizedPnL|Account1
02Orders|Account32Strategies|Account32BuyingPower|Account302CashValue|Account31000002Rea
lizedPnL|Account302OrderStatus|67fd54f568874b969c9087cedbcb0bf3Rejected2Filled|67fd54f56
8874b969c9087cedbcb0bf302AvgFillPrice|67fd54f568874b969c9087cedbcb0bf302OrderStatus|8d9b
9e8aaa0c4c2e8b883f497e0988b1Rejected2Filled|8d9b9e8aaa0c4c2e8b883f497e0988b102AvgFillPri
ce|8d9b9e8aaa0c4c2e8b883f497e0988b102OrderStatus|074893f5ce804a39add9d1483da0d0baRejecte
d2Filled|074893f5ce804a39add9d1483da0d0ba02AvgFillPrice|074893f5ce804a39add9d1483da0d0ba
02Orders|Secret Account2Strategies|Secret Account2BuyingPower|Secret Account02CashValue|
Secret Account2330002RealizedPnL|Secret Account02ATITrue

^C
nitro0us@bukowski:~$
    
```

- Integration with other trading software
 - Including TCP/IP
 - No limit of concurrent sessions
 - Memory exhaustion
- Some listens only in localhost interface
 - XMLHttpRequest () in JavaScript

- **TD Ameritrade's Thinkorswim's TCP-Orders Server**
 - No limit for concurrent connections
 - No waiting time between orders
 - Reverse engineered



NYSE opens in
16 19 10
HOURS MINS SECS

thinkorswim desktop application

thinkorswim desktop application no responde

Windows puede comprobar una solución en línea. Si cierra el programa, podría perder información.

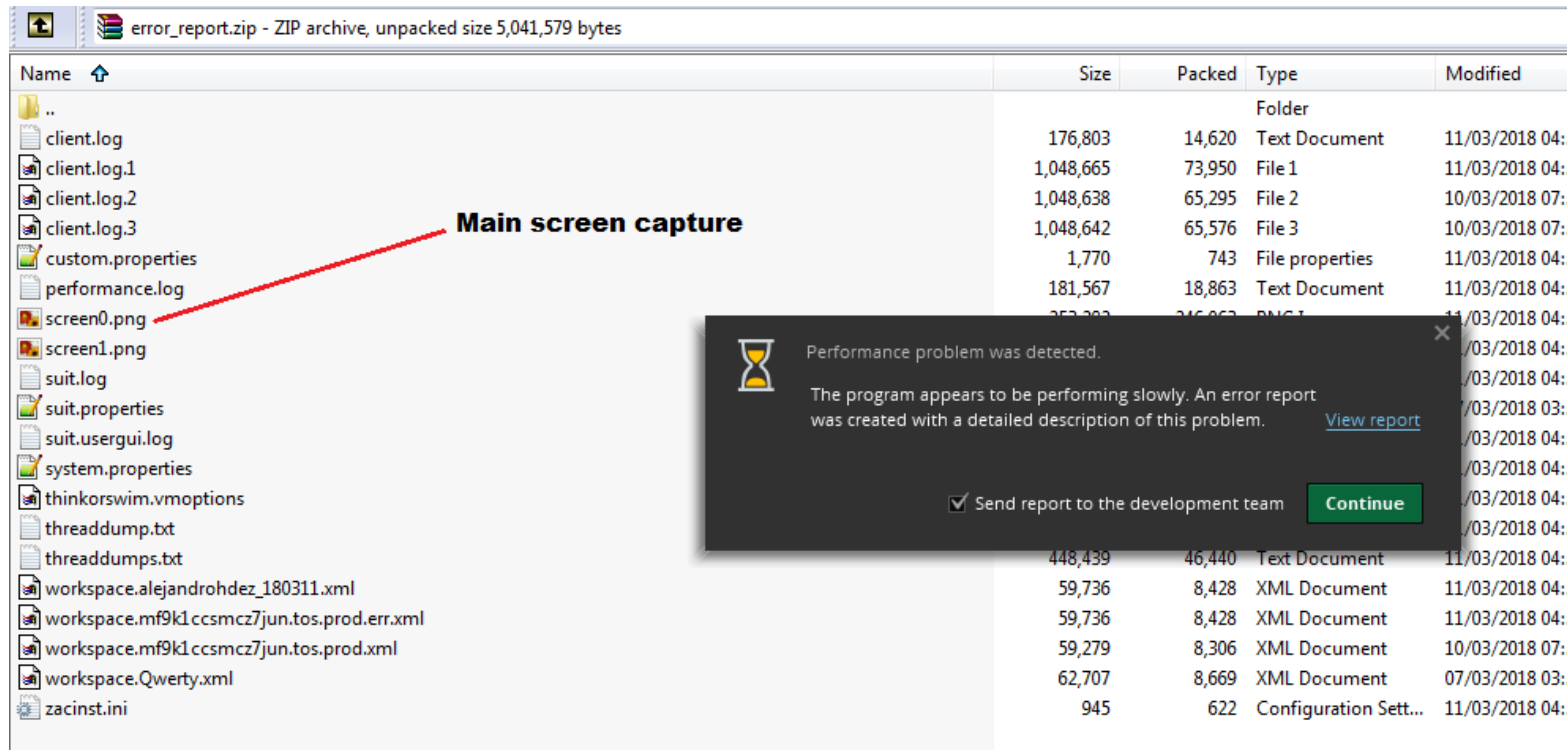
- Compruebe si existe una solución y cierre el programa
- Cerrar el programa
- Esperar a que el programa responda

Ocultar detalles del problema

Descripción:
Este programa dejó de interactuar con Windows por un problema.

Firma con problemas:
Nombre del evento de problema: AppHangB1
Nombre de aplicación: thinkorswim.exe
Versión de la aplicación: 0.0.0.0
Marca de tiempo de la aplicación: 5577fa89
Firma de bloqueo: 9a2d

- **TD Ameritrade's Thinkorswim's TCP-Orders Server**
 - On error, a .zip file including a screenshot is sent to developers
 - Do devs need to know the balances, positions, net worth, etc?



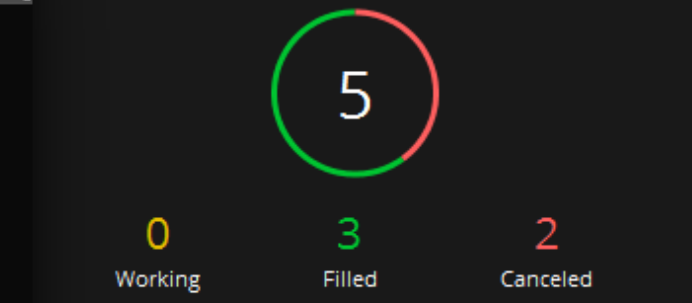


Symbol	Last	Change	High	Low
DXR	13.35	+5.5501	21.66	8.05
OSN	3.10	+0.45	3.30	2.58
JNP	12.50	+1.10	12.65	11.00
INO	4.84	+0.37	4.90	4.29
PTI	7.08	+0.525	8.61	6.82
MHH	14.77	+1.08	15.00	13.76
NES	22.00	+1.58	22.00	20.46

P/L Open
(\$3,584.37) ▾
 (\$0.10) 0.00%



MGA
 MAGNA INTL INC COM
 Last: 56.53
 % Change: 0.0609985
 Market Cap: 20,256 M



- All updates Events
- 2 new updates ↑
 - Mar 22, 2018 10:00 (in 6 days)
 - Econoday event **Baker-Hughes Rig Count**
Mar 16, 2018 10:00 (in 20 hours ...)
 - Econoday event **6-Month Bill Announcement**
Mar 22, 2018 08:00 (in 6 days)
 - Econoday event **3-Month Bill Announcement**
Mar 22, 2018 08:00 (in 6 days)
 - Econoday event **52-Week Bill Announcement**
Mar 22, 2018 08:00 (in 6 days)
 - Econoday event **2-Yr FRN Note Announcement**
Mar 22, 2018 08:00 (in 6 days)

ORDER FOR NFLX (10) LIMIT COST 20000

```
private void parseCommand(String command)
{
    String last = command;
    if ((last = testCommandPrefix(last)) == null)
        throw new IllegalArgumentException();
    if ((last = parseUnderlying(last)) == null)
        throw new IllegalArgumentException();
    if ((last = parseLegs(last)) == null)
        throw new IllegalArgumentException();
    if ((last = parseSuffix(last)) == null)
        throw new IllegalArgumentException();
}

private String testCommandPrefix(String s) {
    if (!(s.startsWith("ORDER FOR ") || ("ORDER FOR ".length() >= s.length())))
        return null;
    return s.substring("ORDER FOR ".length());
}

private String parseUnderlying(String s) {
    int i = s.indexOf(' ');
    if ((i == 0) || (i == -1) || (i + 1 >= s.length()))
        return null;
    this.underlying = s.substring(0, i);
    return s.substring(i + 1);
}

private String parseLegs(String s) {
    int idx = 0;
    if (s.charAt(idx) != '(')
        return null;
    int closure = s.indexOf(')');
    if (closure == -1) {
        return null;
    }
    idx++;
    char ch = s.charAt(idx);
    StringBuilder buffer = new StringBuilder();
    for (;;) {
        int mode = 0;
        TradingServerRAT.Leg leg = new TradingServerRAT.Leg();
        while ((ch != '(') && (ch != ')')) {
            if (ch == '(') {
                if (mode == 1)
                    return null;
                leg.qty = Double.parseDouble(buffer.toString());
                buffer.delete(0, buffer.length());
            }
            else if (ch == ')') {
                mode = 1;
            }
            else {
                buffer.append(ch);
            }
            ch = s.charAt(++idx);
        }
        List symbols = (List)this.legs.get(leg.symbol);
        if (symbols == null)
            this.legs.put(leg.symbol, symbols = new ArrayList());
        symbols.add(leg);
    }
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' ')) {}
    if (idx >= len) {
        return "";
    }
    StringTokenizer tokens = new StringTokenizer(s, " ");
    if ((tokens.hasMoreTokens()) && (!tokens.nextToken().equals("LIMIT"))) {
        return null;
    }
    if (!tokens.hasMoreTokens())
        return null;
    if (!tokens.nextToken().equals("COST")) {
        return null;
    }
    if (!tokens.hasMoreTokens())
        return null;
    this.limit = Integer.parseInt(tokens.nextToken());
    this.limit_order = true;
    return "";
}
```

DEMO

TD Ameritrade's Thinkorswim
Reversed the TCP-order
server. Order pop-up attack.
NULL ptr deref. Error.zip sent
to developers has a
screenshot with balances.

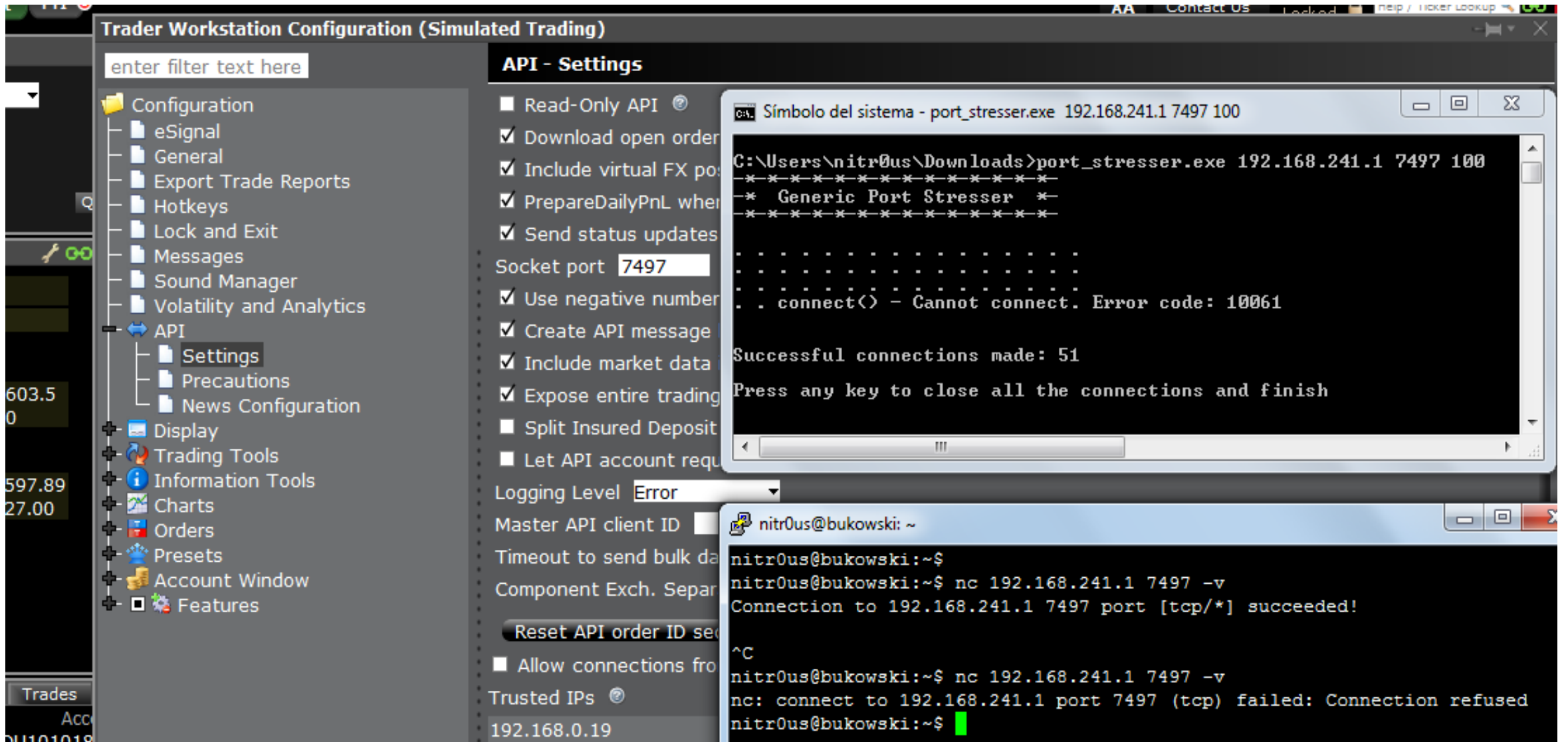
DEMO

eSignal

DoS (memory leak) through
JavaScript. Any other
application that uses this
service will be disconnected
(in this demo is AmiBroker)

- TCP/IP servers should implement
 - Maximum number of connections
- Timeouts on idle connections
- Seconds/minutes between orders
- Such as **Interactive Brokers:**





It's not a **BUG**,
it's a **FEATURE**

- To develop
 - Expert advisors (trading robots)
 - Indicators
 - Advanced charting
 - Etc.
- Based on other languages
 - C++
 - C#
 - Pascal
- Some restrict DLL imports, or warn about them

- **MetaTrader:** MetaQuotes Language
 - Based on C++ - **Supports DLL imports**
- **NinjaTrader:** NinjaScript
 - Based on C# - **Supports DLL imports**
- **TradeStation:** EasyLanguage
 - Based on Pascal - **Supports DLL imports**
- **AvaTraceAct:** ActFX
 - Based on Pascal - Does not support OS commands nor DLL imports
- **(FxPro/IC Markets) cTrader**
 - Based on C# (OS command and DLL support is unknown)

DEMO

The background of the image is a blurred city street at night, with various lights and buildings creating a bokeh effect. In the foreground, there is a server rack with many small, glowing lights in various colors (blue, green, red, yellow).

**MetaTrader
backdoor disguised as an
Ichimoku indicator.**

DEMO



NinjaTrader
Malicious code in a chart
style.

- **Passwords stored unencrypted**

- 3 desktop applications (21%)
- 7 mobile apps (21%)

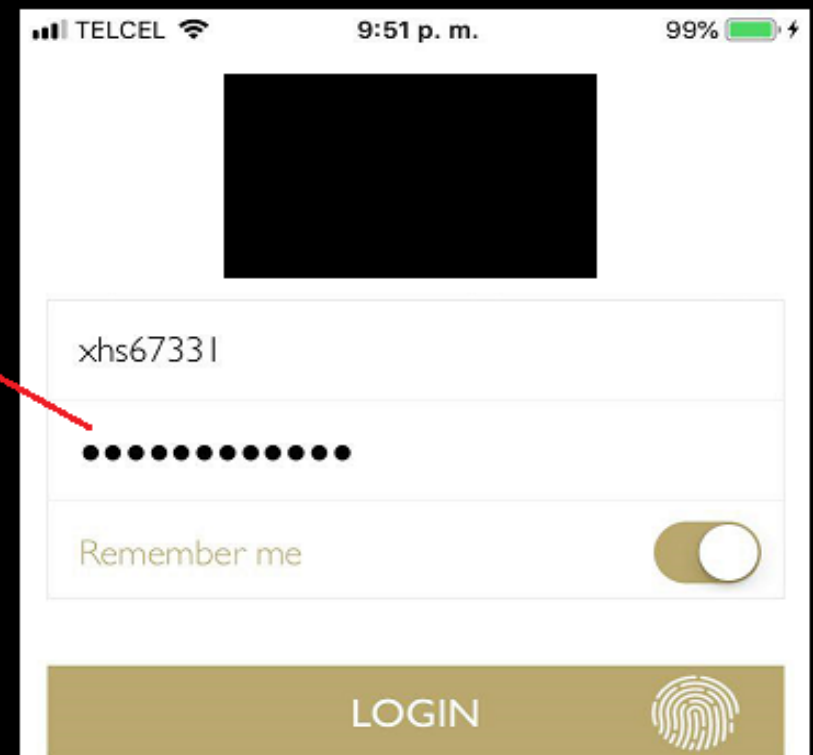
- **Stored unencrypted**

- Configuration file
- Logs
 - File in the fs
 - Logging console
 - `adb logcat`

- *Log in, sell stocks, transfer money to a newly added bank account, delete this bank account, log out.*



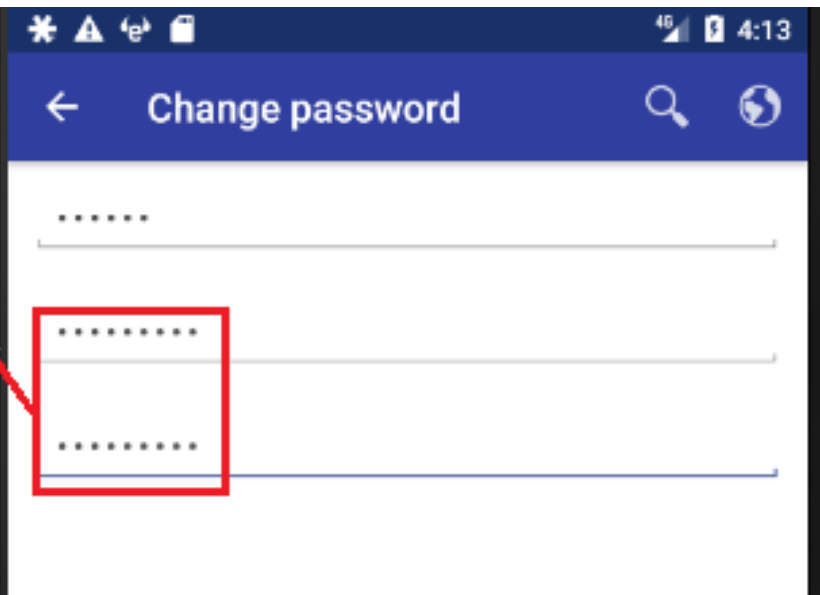

```
nitr0us@bukowski:~/ios/  } plistutil -i Container/Library/Preferences/com. .plist |
egrep -i "userLogin|userPassword" -A 1
  <key>userLoginPlainText</key>
  <string>xhs67331</string>
--
  <key>userPassword</key>
  <string>rCICasboMHL38M8gME0Iox81JrMKoj7if56UN6UDzBXALTYmXrdzw014eB/L7ex3OXJFZG/LhUaAG4bczDeP
EJvLdkxDoui9jB3yFVhlWwHs5sZShKbt1CMGVUncLyPhcbI11x0Jyq753xOSK8IJ8cR44GrorIN0z3vZxcXfh7bCq+enKuHjEvSG
qS2TvH0Fmod8cFTKpwTdA94rzcQYR1ablajqATqGpYGvsPsJz/2FYJV3/qTNwNT508Q73G/famKaHKuUZEUT197r81djZNUR9s8/
Xf9Acnfs5sQVjzPlIc0J0N8KFLFgHtCnR8oS9bIB8OCela+CWCdT4wG9sQ%e%q%e%q</string>
--
  <key>userLoginPlainText</key>
  <string>xhs67331</string>
  <key>userPasswordPlainText</key>
  <string>Qwertyf00b4r</string>
--
  <key>userLogin</key>
  <string>uTkLGmo6PsHflagr+izXDtvyZ7tjU/DV6HnUOvAj7Dw%e%q</string>
nitr0us@bukowski:~/ios/  } █
```



```
per: finishComposingText on inactive InputConnection
input. Cursor position = 0,0
sts received onNext
: KeepAlive
input. Cursor position = 0,0
per: finishComposingText on inactive InputConnection
Window size has been changed. This may cause jankiness of resizing

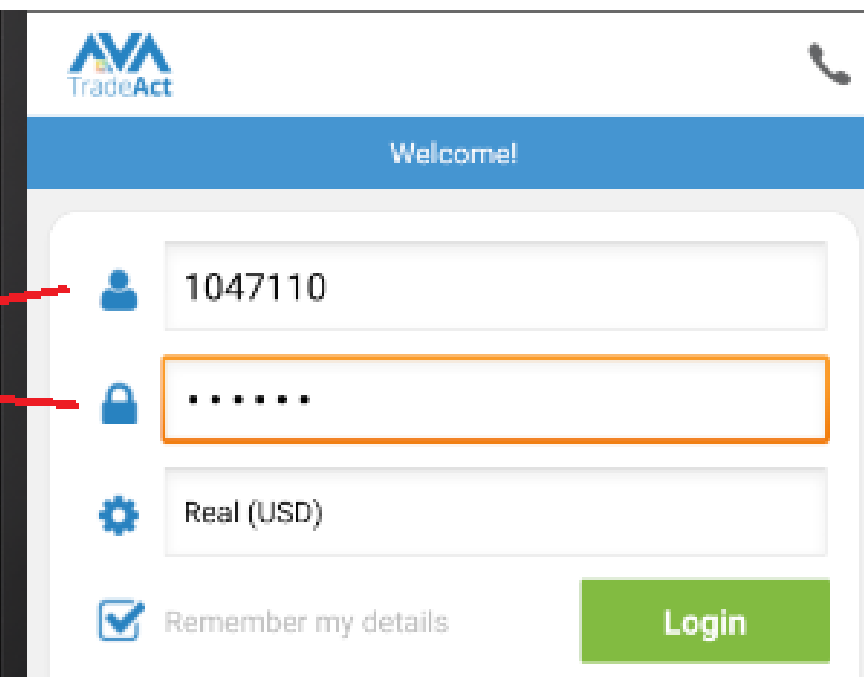
logins.ChangePassword: submit started. newPassword: Qwertyf00
0xb4a83500) throttle end: throttle tim.(38)
ssDialog with keepKey = NetworkCall changePassword b3e125cb-30dc

ssDialogAux: isForeground=true isProgressDialogNotExists=true
loc_alloc: format 1 and usage 0x900 imply creation of host color
loc_alloc: format 1 and usage 0x900 imply creation of host color
loc_alloc: format 1 and usage 0x900 imply creation of host color
ompleted, class=
gressDialog dismiss the key=NetworkCall changePassword b3e125cb-3
```



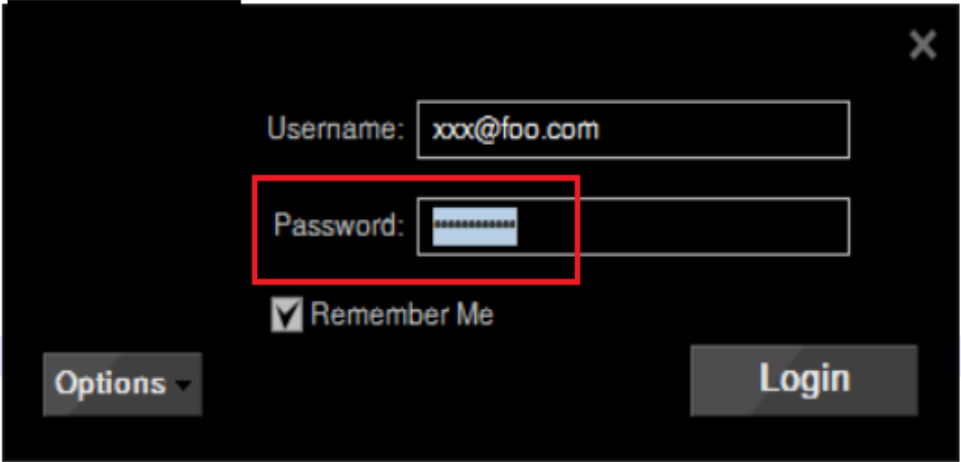
```
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
AudioFlinger: mixer(0xb0103a00) throttle end: throttle tim
DebugMessages: start login
ApiRec : logout()
ApiRec : Can not execute request while status is offline.
ApiRec : login(deal.35, 1047110, P5DJK2, ...
ApiRec : UserAgent: AvaltradeHct 2.3.36(85)(Android SDK bu

DataContainer: setStatus(STATUS_CONNECTING)
ApiDataContainer: doLogin(http://real6.sysfx.com:8035/xml/
ApiDataContainer: login()
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
LayoutMethodService: hideView has been shown. This view
```



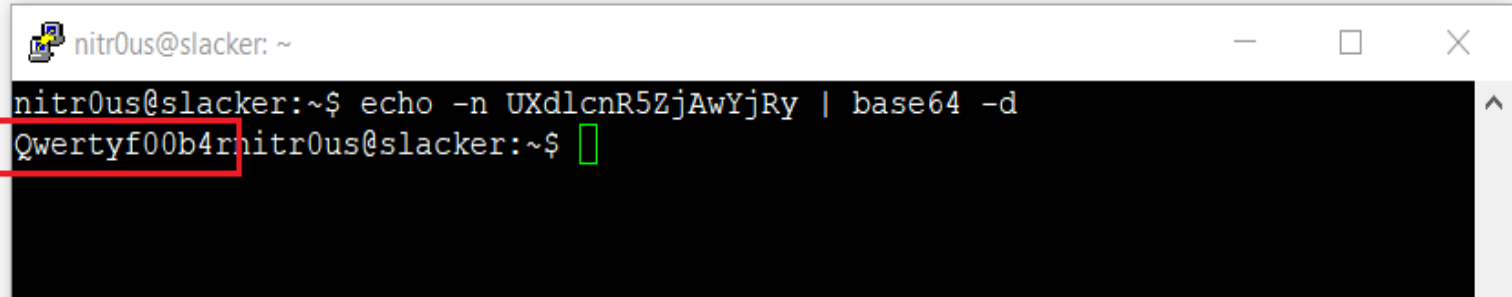
Base64 != encryption

```
1 #Sat Jul 28 17:15:45 CDT 2018
2 boundsH=799.0
3 frame=2
4 websocket=false
5 boundsY=-8.0
6 boundsX=-8.0
7 boundsW=1552.0
8 username=xxx@foo.com
9 version=1.4
10 proxy=false
11 password=UXdlcnR5ZjAwYjRy
12 zoom=1.0
13 storeInto=1
14
```



A screenshot of a login form with a dark background. The form contains a 'Username' field with the value 'xxx@foo.com', a 'Password' field with a masked password, and a 'Remember Me' checkbox which is checked. There are 'Options' and 'Login' buttons at the bottom. A red box highlights the password field.

```
nitr0us@slacker: ~
nitr0us@slacker:~$ echo -n UXdlcnR5ZjAwYjRy | base64 -d
Qwertyf00b4rnitr0us@slacker:~$
```



A terminal window showing the command `echo -n UXdlcnR5ZjAwYjRy | base64 -d` being executed. The output is `Qwertyf00b4rnitr0us@slacker:~$`. A red box highlights the output text.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name=".key_last_mode">auth</string>
  <long name=".key_last_event_timestamp" value="1528410163273" />
  <string name=".key_last_user_account">21022981</string>
  <string name=".key_last_crm_user">{"&quot;Accounts&quot;: [{"&quot;AdditionalData&quot;: {}, &quot;AccountCrmGuid&quot;: &quot;1759407&quot;, &quot;Currency&quot;: &quot;USD&quot;, &quot;AccountID&quot;: &quot;21022981&quot;, &quot;ServerName&quot;: &quot;demo&quot;, &quot;AccountType&quot;: &quot;Demo&quot; }], &quot;Email&quot;: &quot;[REDACTED]&quot;, &quot;Token&quot;: &quot;iMxKHJVv7Wdf8nvHNwdBTWBdb0j11uswR6ekkT11414HeTSuASp0JKpwc88y5NvrDnmtPz9YuxMNsoFLNzwI9CiBnRRr4y3rJwfbvXD0%2bdBmTibLeVC46BnlkSbYd9mIgrV%2bYeyQv51vRElh5dQG1HOjNz1ts9SHrc71BS%2b%2fdMPsJCmE7VID6C7OZxJsZevzW4P0vJeF6w1P5DCz1UYWyRGWuOFJBHsAhMX6XHSafcA7BI1XbhjrjKAAidvJ67E7FwWUzRLs%3d&quot;}</string>
  <string name=".key_crm_credentials">{"&quot;credentialsTO&quot;: {"&quot;credentialsType&quot;: {"&quot;name&quot;: &quot;REGULAR&quot;, &quot;ordinal&quot;: 0}, &quot;login&quot;: &quot;[REDACTED]&quot;, &quot;password&quot;: &quot;6ynH26rP&quot;}, &quot;expirationDate&quot;: 1529618798765}</string>
</map>
```

Burp Suite Professional v1.7.33 - Temporary Project - licensed to IOActive [46 user license]

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder
Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

<string name=".key_crm_credentials">{""credentialsTO": {""credentialsType": {""name": "REGULAR", "ordinal": 0}, "login": "[REDACTED]", "password": "6ynH26rP", "expirationDate": 1529618798765}</string>

Text Hex ?
Decode as ...
Encode as ...
Hash ...
Smart decode

Text Hex
Decode as ...

Search <Ctrl+K>

Filter these messages <Ctrl+Shift+K>

Reply Forward Archive Junk Delete More

From AvaTrade <Customer@avatrade.com> ☆

Subject **Welcome to AvaTrade – Your Demo Account** 07/06/2018 03:49 p.m.

Information

To Me <[REDACTED]> ☆

To enter the MetaTrader4 demo platform:

Login: 21022981

Server: Ava - Demo

Password: 6ynH26rP

Choose your way to access the platform:

PC Web Trading Google Play Apple Store

Unread: 0 Total: 833

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="password">Qwertyf00</string>
  <string name="cache.url.csprodlive">live-trader-mob12.markets.com:443</string>
  <string name="last.server.address">live</string>
  <long name=".authStartTime" value="1529451161870" />
  <boolean name=".first_launch" value="false" />
  <string name="firebase_instance_token_key">d0uzkIqO19M:APA91bHeZ7mvHECKjnMHrri3Ng_uLBFzfA0p2gwL4u6f
WvUA5vG5BjgLiFWqEfQZEYDh39nXxvdBluSFEqVLrY-NRyOHY19Mg</string>
  <string name="last.server.key">MarketsProd</string>
  <string name="PREF_KEY_MANDATORY_UPDATE_LINK">https://play.google.com/store/apps/details?id=com.ma
  <string name="r              :@gmail.com quotes">AmericaMovil|Cemex|Medtronic|TESLA|GoPro|</string>
  <int name="PREF_KEY_LATEST_SELECTED_TAB" value="3" />
  <string name="n              :@gmail.com.ChartSavedState">&lt;?xml version='1.0' encoding='UTF-8' sta
ey=&quot;CHART_ID&quot; value=&quot;173873340&quot; /&gt;&lt;string key=&quot;edit_index&quot; value=&
t;true&quot; /&gt;&lt;bundle key=&quot;0.parameters.bundle&quot;&gt;&lt;string key=&quot;parameters.co
quot;autoposition_mode&quot; value=&quot;true&quot; /&gt;&lt;string key=&quot;.fitVertical&quot; value
value=&quot;false&quot; /&gt;&lt;string key=&quot;show.indicators&quot; value=&quot;true&quot; /&gt;&lt;
```

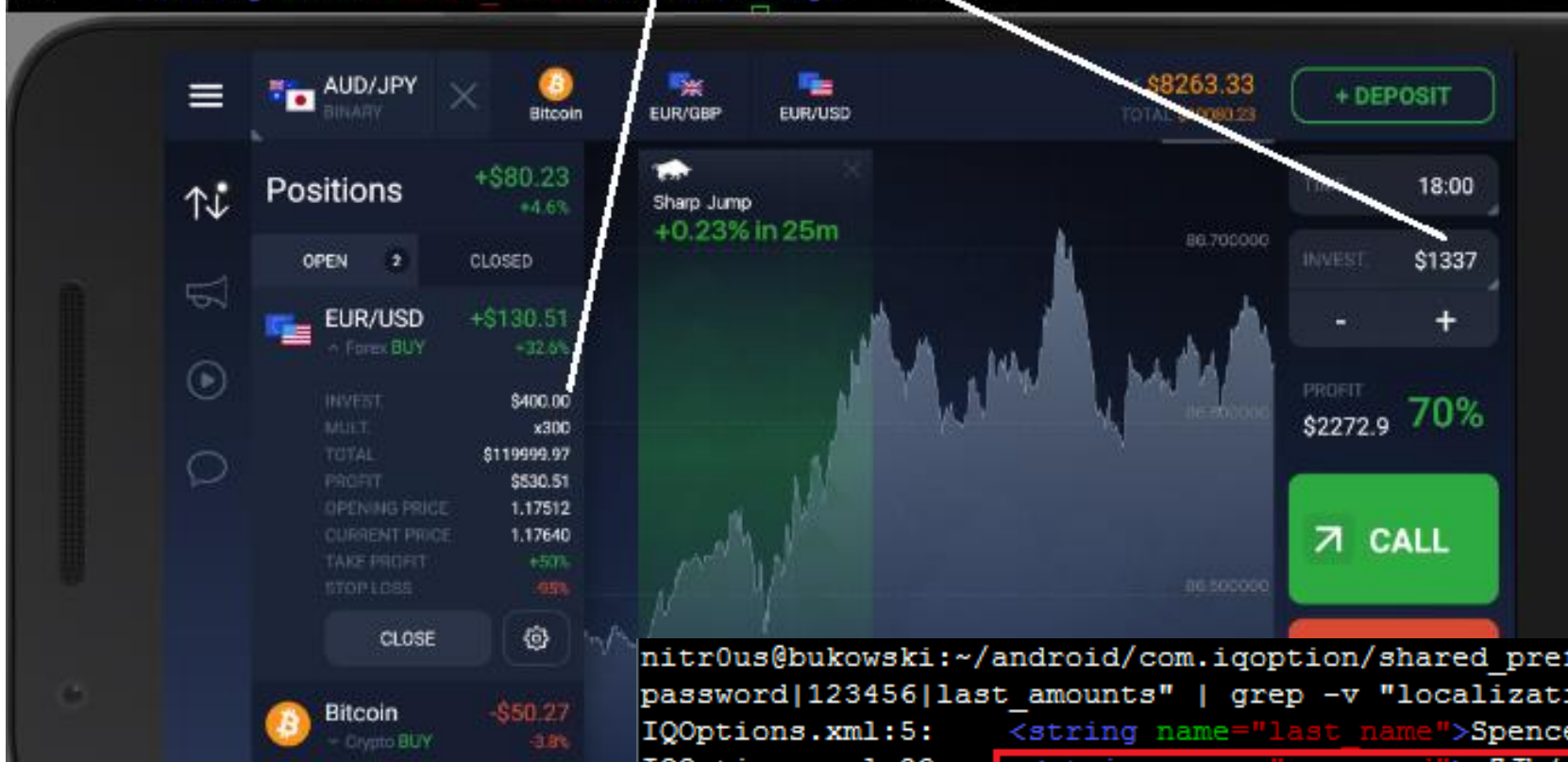
```
owski:~/ios/... $ sqlite3 "Container/Library/Application Support/
select * from _____"
|0|0|0|0|0|0|0|0|1|1|1|1|914347700.631725|4eb4961a8bec044e07bd42b255dfce89a181714e2aaea3
5124cc6|MX|Mexico|...@gmail.com|https://www. /join/5b48dc40bec71
|John Spencer|MXN|1739|7ac53fdcaea9afe090910307485604a7b360f2ec2009a647bb4bc12f926e83
0-9426-5634-8507-eded4f8afla7|bplist00||efX$versionX$objectsY$archiverT$top
s@bukowski:~/ios/... $
```



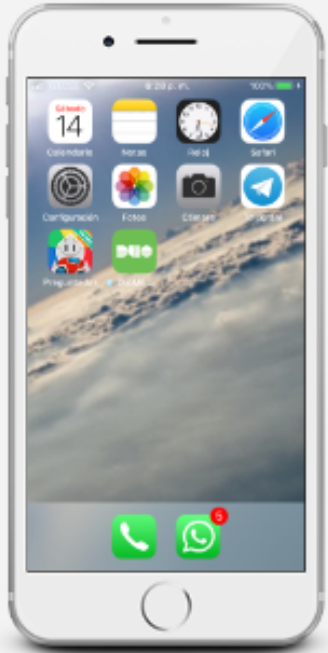
Unlock with your PIN



```
nitr0us@bukowski:~/android/com      $ egrep -nir "      |john|spencer|Qwerty|1337"
hared_prefs/      :.xml | grep -v localization_json | source-highlight -f esc -s xml
5:      <string name="last_name">Spencer</string>
24:      <string name="password">Qwertyf00b4r</string>
29:      <string name="email">      :@gmail.com</string>
34:      <string name="last_amounts">[400.0 1337.0 10.0]</string>
44:      <string name="first_name">John</string>
```



```
nitr0us@bukowski:~/android/com.iqoption/shared_prefs$ egrep -nir "john|spencer|n:      }r|
password|123456|last_amounts" | grep -v "localization_json" | source-highlight -f esc -s xml
IQOptions.xml:5:      <string name="last_name">Spencer</string>
IQOptions.xml:23:      <string name="password">-ZJh(!@3dGfQ9W86</string> -- encrypted
IQOptions.xml:27:      <string name="email">n      :c@gmail.com</string>
IQOptions.xml:40:      <string name="first name">John</string>
app_pref_name.xml:10:      <string name="two step auth password">123456</string>
app_pref_name.xml:14:      <string name="two_step_auth_user">n      }r@gmail.com</string>
app_pref_name.xml:17:      <string name="login_email">      :@gmail.com</string>
nitr0us@bukowski:~/android/com.iqoption/shared_prefs$ █
```

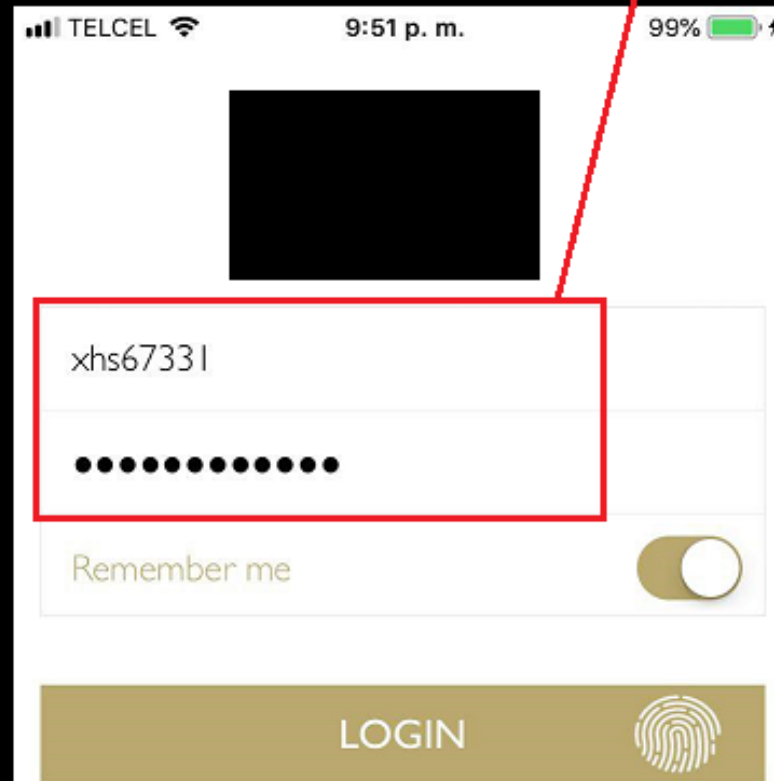


DETALLES DEL DISPOSITIVO:



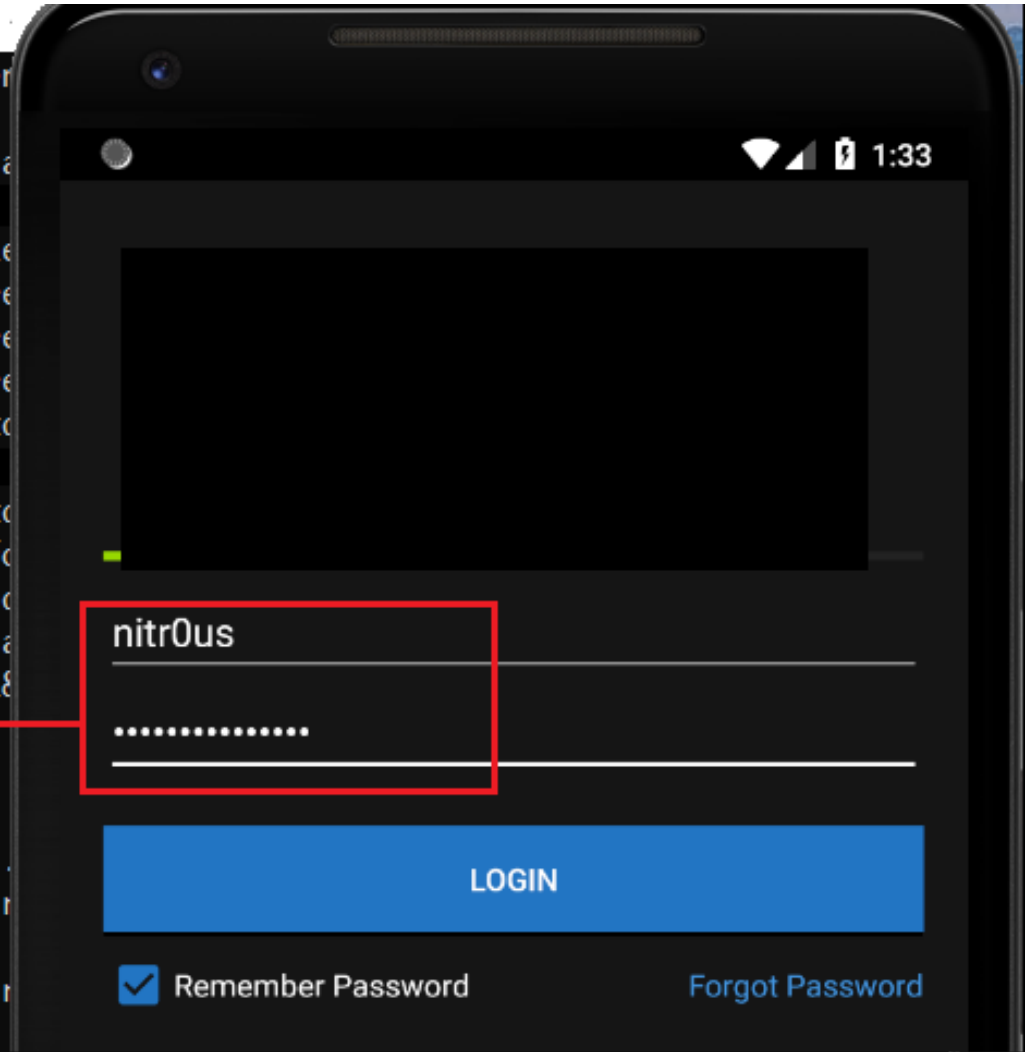
- iPhone 6 - iOS 11.4
- 18/07/2018 09:38 p. m.
- 7 copia(s) de seguridad
- DANGER (C:) (34.67 GB)
- @ [Redacted]
- +52 (55) [Redacted]

```
Jul 18 21:35:13 iPhone [452] <Notice>: Logging URL: https://trade. /common/  
frontend/public/login.aspx?mobile=true&username=xhs67331&password=Qwertyf00b4r  
Jul 18 21:35:13 iPhone [452] <Notice>: Logging URL: https://trade. /common/  
frontend/public/login.aspx?mobile=true&username=xhs67331&password=Qwertyf00b4r
```



Administrator: Símbolo del sistema - adb logcat

```
07-15 01:32:55.577 1414 3454 W audio_hw_generic: Not supplying er
nly wrote 3007440
07-15 01:32:55.602 1432 1432 D SurfaceFlinger: duplicate layer na
e
07-15 01:32:55.603 5640 6753 D Volley : [262] DiskBasedCache.cle
07-15 01:32:55.614 1422 1422 D gralloc_ranchu: gralloc_alloc: Cre
07-15 01:32:55.637 1422 1422 D gralloc_ranchu: gralloc_alloc: Cre
07-15 01:32:55.650 1422 1477 D gralloc_ranchu: gralloc_alloc: Cre
07-15 01:32:55.700 5640 5683 D EGL_emulation: eglMakeCurrent: 0xc
07-15 01:32:56.168 5640 5683 I chatty : uid=10083(
07-15 01:32:56.208 5640 5683 D EGL_emulation: eglMakeCurrent: 0xc
07-15 01:32:56.228 5640 6755 E Volley : [264] BasicNetwork.perfo
ps://
de&connection type=WIFI&device type=Android&client_type=MOBILE&loc
=Android&password=sup3rs3cr3t%21%21%21%21&api_key=68e9c4cec7792f228
ient_version=5.5.2&username=nitr0us
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: statusCode:
.oanda.com1531618377986
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: com.android.
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: at com.and
BasicNetwork.java:142)
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: at com.and
her.java:110)
```



New Window IBot FYI

AA Contact Us Layout Locked Help / Ticker Lookup

Order Entry

AMZN 1602.50 1603.50 Adaptive Option Chain

BID MID ASK

BUY SELL QTY 100 LMT LMT PRICE 0.00 DAY advanced

Complete your Application

Ready to Start Trading?

Experience our best price execution and generate higher

AMZN 1603.45

-5.63 -0.35%

Last Size 1
Last Exch
Bid/Ask 1602.5 x 1603.5
Size 37 x 10
Ask Exch
Bid Exch
Hi/L
52 H
EAR



C:\Uts\heojhcohbefemofkedbpaiefmfjihppfadgbmajfm\tws.Sat.xml - Notepad++

```

Archivo  Editor  Buscar  Vista  Codificación  Lenguaje  Configuración  Macro  Ejecutar  Plugins
Ventana  ?
tws.Sat.xml
21831  <ESignalSettings varName="esignal" allowed="true"
        username="myeSignalUsername" password="s3cr3t" host=
        "CM*.esignal.com" throttlingPace="1" apiUnpacedUpdates=
        "true">
21832  <sigtext></sigtext>
21833  <ESignalSecSettings varName="opt">
21834  <ESignalExchangeSettings varName="usa" top=
        "true" depth="true" hist="false"/>
length: 192440 Ln: 21831 Col: 11 Sel: 0 | 0 UNIX UTF-8 w/o BOM INS
  
```

Trader Workstation Configuration (Simulated Trading)

enter filter text here

- Configuration
 - eSignal
 - General
 - Export Trade Reports
 - Hotkeys
 - Lock and Exit
 - Messages
 - Sound Manager
 - Volatility and Analytics
 - API

Some options are hidden...

eSignal

Use eSignal for Market Data*

Connectivity*

User name: myeSignalUsername

Password:

Host Address: CM*.esignal.com

SigText directory: _____

Update frequency

Updates per second: 1

Non-paced updating for API:

OK Apply Cancel

Proxy settings

Use a proxy server

Address

192.168.1.254

Port

31337

Username

proxy_user

Password

.....

```
nitr0us@ubuntu: ~/.local/data/IQ Option
nitr0us@ubuntu: ~/.local/data/IQ Option$ more cfg.dat
{"ssid":"","user_id":21519658,"locale":"C","user_locale":"en_US","remember_login":true,"login":"nitrousenador@gmail.com","token":"","tokenHost":"iqoption.com:443","show_lowfps_notice":true,"user_agent":"","device_id":"FBEEBDACE-6C5C-CA91-A8F2-817A1D9CB78","theme":"blue","theme_plot_bg_visibility":true,"login_plot_mode":"area","login_regulator_logos":false,"proxy_use":true,"proxy_address":"192.168.1.254","proxy_port":"31337","proxy_login":{"proxy_user":"proxy_user","proxy_password":"s3cr3t"}}
nitr0us@ubuntu: ~/.local/data/IQ Option$
nitr0us@ubuntu: ~/.local/data/IQ Option$
```

AvaTradeAct

HTTP Proxy Settings

Use Proxy

Server: 192.168.1.1 Port: 8080

Login: myproxy

Password:

Alternate Configuration Server

Server: alternate-server.mycompany.com Port: 1337

C:\Program Files (x86)\AvaTradeAct\user_loader_settings.xml - Notepad++

```
<?xml version="1.0" encoding="utf-8"?>
<user_loader_settings client_id="" last_login="bukowski31337" last_entry="Real (USD)" language="en_US" skin="Dark" password="Z0C84X8qOEOYX21k03GuZphK0s97hhB3+HqW8Q/f1RJGZpp+39/pXNoe0gu0">
  <proxy enabled="true" server="192.168.1.1" port="8080" login="myproxy" password="s3cr3t"/>
  <alternate_server server="alternate-server.mycompany.com" port="1337"/>
</entries>
```

- **Trading data stored unencrypted**

- 8 desktop applications (57%)
- 15 mobile apps (44%)

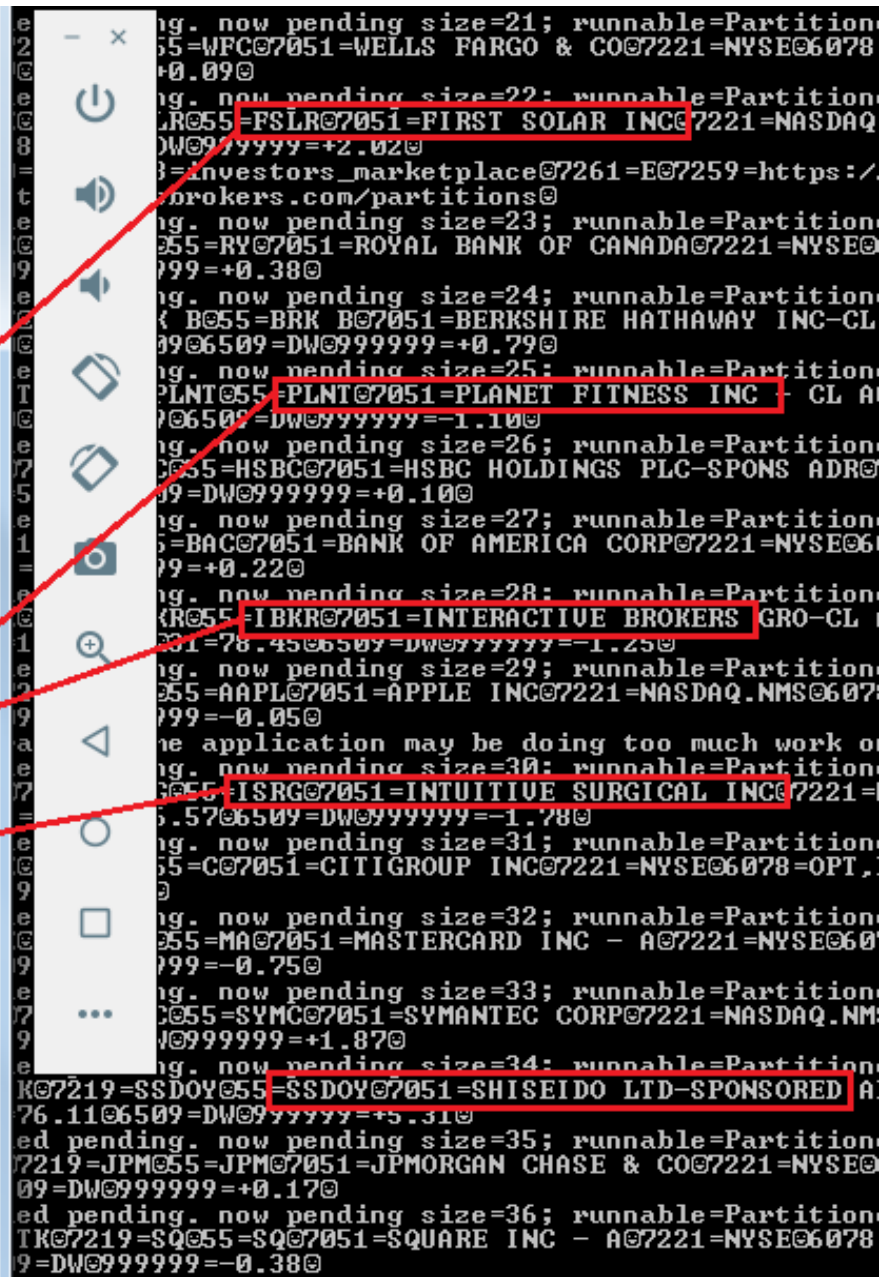
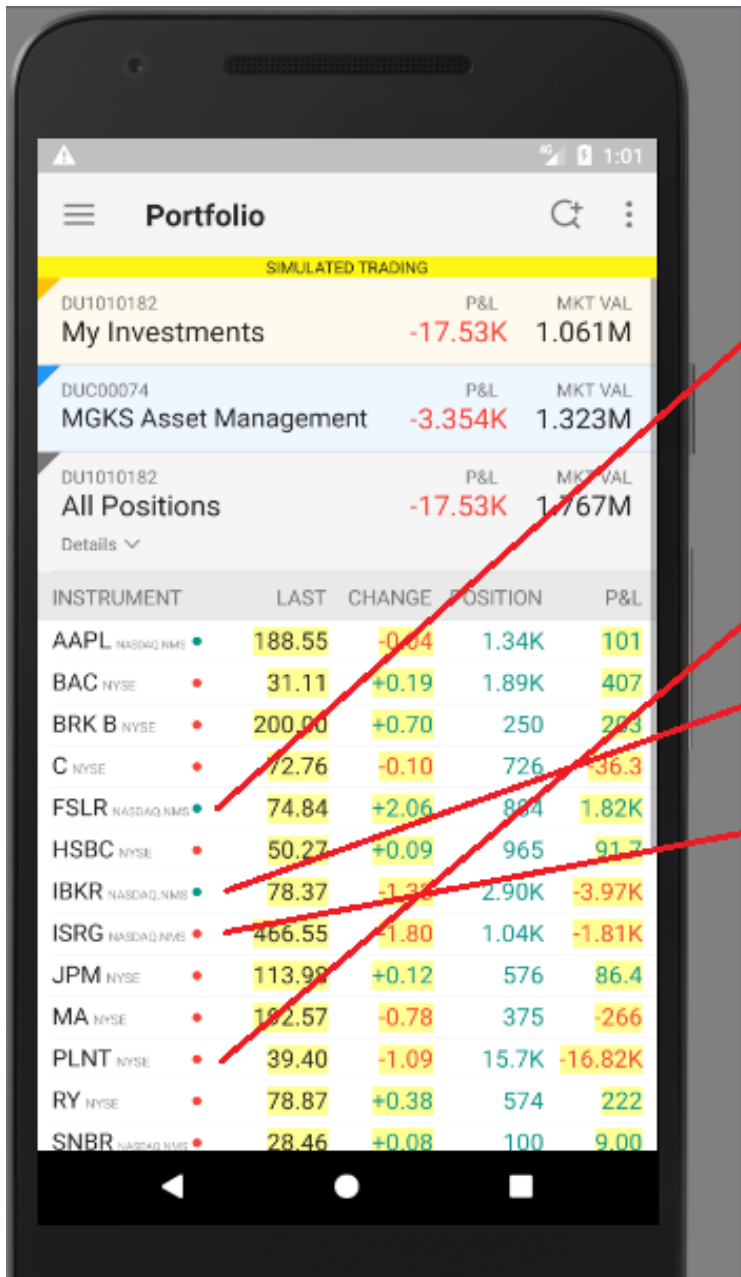
- **Stored unencrypted**

- Configuration file
- Logs
 - File in the fs
 - Logging console
 - `adb logcat`

- *A malicious user could gain insight into users' net worth and investing strategy.*



- **Trading data stored unencrypted**
 - Balances
 - Portfolio
 - Personal data
 - Buy/sell orders
 - Watchlists
 - Quoted symbols
 - Other data



```
I System.out: <liabilityExists>N</liabilityExists>
I System.out: <singleBrkg/>
I System.out: <Funded/>
I System.out: <hasLoyalAccts>NO</hasLoyalAccts>
I System.out: <AssetValue>$0.00</AssetValue>
I System.out: <FmtLgrBankBalance/>
I System.out: <liabilityOnly>NO</liabilityOnly>
I System.out: <hasBrkgAccts>YES</hasBrkgAccts>
I System.out: <LedgerValue/>
I System.out: <hasOLAccts>NO</hasOLAccts>
I System.out: <isGDCEnabled>YES</isGDCEnabled>
I System.out: <singleBrkgSecMrkVal/>
I System.out: <singleBrkgCash/>
I System.out: <hasBankAccts>NO</hasBankAccts>
I System.out: <PDTRiskWarnMsgFlag/>
I System.out: <PDTRiskErrorMsgFlag/>
I System.out: <PDTMessages/>
I System.out: <AccountList>
I System.out: <TotalAvailableForWithdrawal>$0.00</TotalAvailableForWithdrawal>
I System.out: <CashAvailableForWithdrawal>$0.00</CashAvailableForWithdrawal>
I System.out: <MarginAvailableForWithdrawal>$0.00</MarginAvailableForWithdrawal>
I System.out: <MarginLevelCd>1</MarginLevelCd>
I System.out: <DtStatusCd>1</DtStatusCd>
I System.out: <IntradayMargin>$0.00</IntradayMargin>
I System.out: <IntradaynonMargin>$0.00</IntradaynonMargin>
I System.out: <AccountRestrictionLevel>null</AccountRestrictionLevel>
I System.out: <BalCount/>
I System.out: <BuyingPower>$0.00</BuyingPower>
I System.out: <AccountMode>CASH</AccountMode>
I System.out: <AccountDesc>INDIVIDUAL</AccountDesc>
I System.out: <AccountNo>3754-4142</AccountNo>
I System.out: <AccountValue>$0.00</AccountValue>
I System.out: <AccountDescType>INDIVIDUAL</AccountDescType>
I System.out: <LedgerAccountValue/>
```

12:45

Balances

Net Assets **\$0.00**

Individual Brokerage -4142	→
Net Account Value	\$0.00
Available for Withdrawal	\$0.00
Cash Purchasing Power	\$0.00

[View Portfolio](#)

```
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"EntityType":"AccountBalance","CashBalance":"0","PendingCash":"0","PendingOrdersCount":"0","A
}, {"Name\":\"netCash\",\"Value\":907669.390000000000000000000000}, {"Name\":\"excess\",\"Value\":907669.3
000}, {"Name\":\"changePercent\",\"Value\":-0.00454598000000}, {"Name\":\"equityTotal\",\"Value\":999954
tLiquidity\",\"Value\":92285.15020000000000000000}, {"Name\":\"availableCash\",\"Value\":907669.39000000
00}, {"Name\":\"stockShortMarketValue\",\"Value\":0}, {"Name\":\"optionLongMarketValue\",\"Value\":0}, {"
Value\":0}, {"Name\":\"forexShortMarketValue\",\"Value\":0}, {"Name\":\"dayTrades\",\"Value\":0}, {"Name
r\",\"Value\":907669.390000000000000000000000}, {"Name\":\"forexBuyingPower\",\"Value\":907669.3900000000
ingCash\",\"Value\":0}, {"Name\":\"maintenanceMargin\",\"Value\":0}, {"Name\":\"optionMaintenanceMargin
\":\"closePL\",\"Value\":0}, {"Name\":\"market
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
STREAMER: {"Cmd":"Ping","StatusCode":"Ok"}
```



```
22:%222017-08-02T16:08:52.7757946-04:00%22%7D,%22History%22:%7B%22Items%22:%5B%5D,%22TransactionCount%22:0,%22TimeStamp%22:%222017-08-02T16:08:52.7435701-04:00%22%7D,%22Positions%22:%7B%22MoversOrHoldings%22:%5B%5D,%22Items%22:%5B%5D,%22Cash%22:0,%22
2017-08-02T16:08:52.7689591-04:00%22%7D,%22wsodToken%22:%22XXX108_U6+ZELV63gPiA4xEaHq1GHfxLrfe8EJSD3kRwe9185Y22bJNjnL/wM1K3VS2rD3/
Aug 2 15:08:53 Polaris Schwab(CScoreMobileUtilities)[1201] <Notice>: #iOS#{"data":{"AccountId":"82195828","AccountDetails":
{"AccountNickName":"Individual","IsBrokerageAccount":true},"Balance":
{"TotalBalance":0,"AvailableBalance":0,"AccountCashBalance":0,"AccountMarketValue":0,"CashPercent":0,"MarketValuePercent":0,"TotalDayChange":0,"TotalD
":true,"TimeStamp":"2017-08-02T16:08:52.7748181-04:00"},"OrderStatus":
{"Open":0,"Filled":0,"Cancelled":0,"Todays":0,"OrderCount":0,"HasData":true,"TimeStamp":"2017-08-02T16:08:52.7757946-04:00"},"History":{"Items":
[],"TransactionCount":0,"TimeStamp":"2017-08-02T16:08:52.7435701-04:00"},"GainLoss":{"TimeStamp":"2017-08-02T16:08:52.7425936-04:00"},"Positions":{"Mov
[],"Cash":0,"TimeStamp":"2017-08-02T16:08:52.7689591-04:00"},"wsodToken":"XXX108_U6+ZELV63gPiA4xEaHq1GHfxLrfe8EJSD3kRwe9185Y22bJNjnL/wM1K3VS2rD3/
1j)ETMZZNB5TXW0K1T0SxQ0Eav000C","TimeStamp":"2017-08-02T16:08:52.8055721-04:00"},"Status":"200","Config":{"method":"GET","transformRequest":[null],"tr
[null],"url":<\M-b\M^@\M-&>
```

```

119=Q22@7091=32769@7036=0@7094=-22@ACCOUNT@6119=Q19@7091=32769@7036=0@7094=-23@AC
COUNT@6119=Q20@7091=32769@7036=0@7094=-20@ACCOUNT@6119=Q25@7091=32769@7036=0@7094
=-21@ACCOUNT@6119=Q18@7091=32769@7036=0@10=164@
08-11 13:13:09.773 3098 3115 I aTws : [main]: ActivityState:<atws.activity.p
ortfolio.PortfolioActivity@71d3334>.onAttachedToWindow()
08-11 13:13:09.833 3098 3115 I aTws : [IN-0-0]: 35=u@6040=R@320=5616@108=300
0@7098=500@
08-11 13:13:10.139 3098 3115 I aTws : [IN-0-0]: 35=P@6040=S@320=20709905=509
081-006119-007094-448072=1.337076=1.34K@73=24194.35075=2.6706070=STK@7219=AMX@55
=AMX@7051=AMERICA MOVIL-SPN ADR CL L@7221=NYSE@7039=106119=107091=158219582@72=50
0076-500073-1075-00075-2.00@6070=STK@7219=GPRO@55=GPRO@7051=GOPRO INC-CLASS A@72
21=NASDAQ.NMS@7039=106119=207091=70702221@72=446076-116073-152131-62075=-32.85@60
70=STK@7219=TESLA@55=TESLA@7051=TESLA INC@7031=NASDAQ.NMS@7039=106119=307094=BASE@7
3=811K@55=BASE@7158=160@119=407094=USD@73=811K@55=USD@7158=160
08-11 13:13:10.530 1566 1587 I ActivityManager: Displayed atws.app/atws.activit
y.portfolio.PortfolioActivity: +1s612ms
08-11 13:13:11.444 3098 3115 I aTws : [main]: ActivityState:<atws.activity.n
avmenu.NavMenuBlankActivity@e3f764f>.onSaveInstanceState()
08-11 13:13:11.486 3098 3115 I aTws : [main]: ActivityState:<atws.activity.n
avmenu.NavMenuBlankActivity@e3f764f>.onStop() saved=true
08-11 13:13:11.506 3098 3115 I aTws : [main]: ActivityState:<atws.activity.t
rades.TradesActivity@9711f84>.onStop() saved=false
08-11 13:13:11.507 3098 3115 I aTws : [main]: ActivityState:<atws.activity.t
rades.TradesActivity@9711f84>.onDestroy()

```

ACCOUNT	P&L		Net Liq		
DU777918	117		1M		
ExLiq	952.9K	SMA	905.8K	Unrlz	71.00
MntMgn	47.16K	BuyPwr	3.811M	Rlzd	0.00
INSTRUMENT	LAST	CHG	POS	P&L	
AMX NYSE	18.12	+0.21	1.34K	34.8	
GPRO NASDAQ NMS	9.81	+0.03	500	7.50	
TSLA NASDAQ NMS	357.71	+2.31	446	74.4	
TOTAL Cash	811K (Market Value)				
USD Cash	811K (Market Value)				

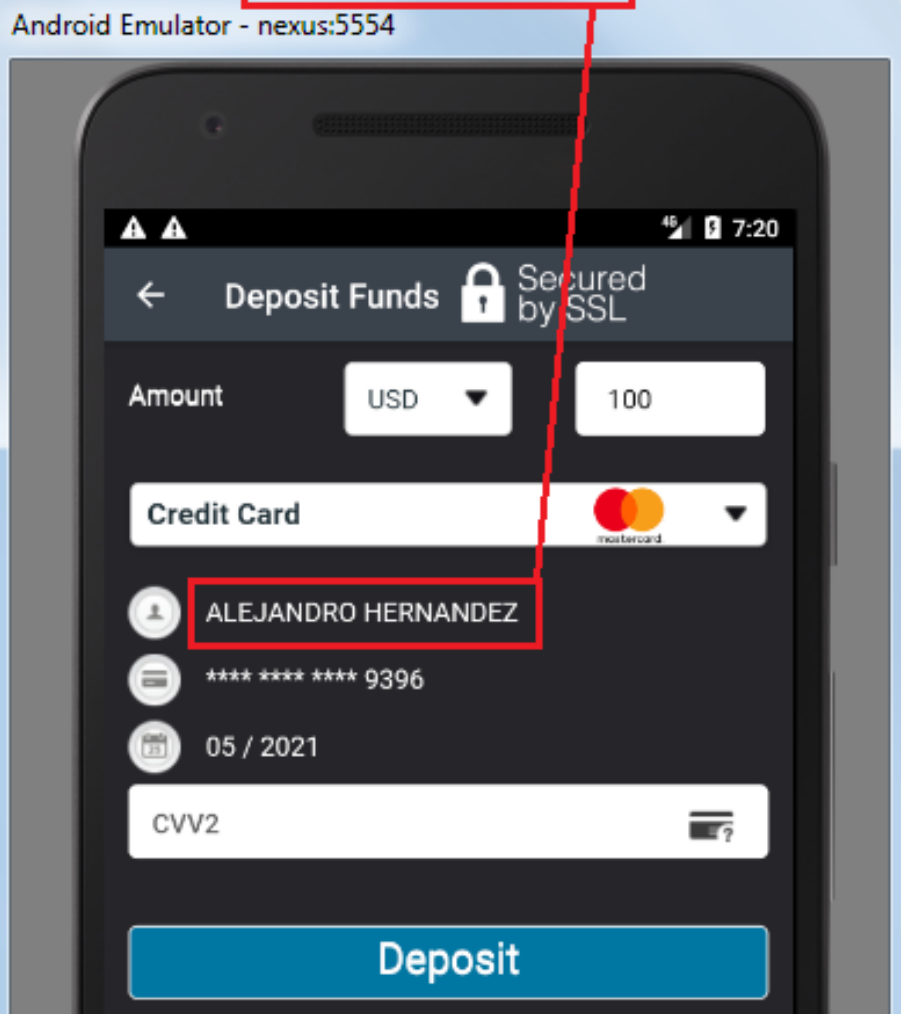
```

6, "demoCID": 8134981, "username": "bukowski31337", "firstName": "John", "lastName": "Spencer", "playerLevel": 1, "gender": 1, "language": 6
, "dateOfBirth": "1929-09-11T00:00:00.000Z", "contactUserInfo": {"gcid": 7078031, "country": 132, "countryByIp": 132, "province": 3848, "
provinceByIp": 3848, "email": "nitrousenador@gmail.com", "address": "Street Fighter 1337", "city": "Mexico City", "zip": "31337", "phone
": "5511111337", "phonePrefix": "52", "phoneBody": "5511111337", "mobile": null, "fax": null, "buildingNumber": "123", "state": 0, "riskUse
rInfo": {"gcid": 7078031, "regulatingEntity": 5, "documentStatus": null, "phoneVerificationStatus": 1, "verificationLevel": 2, "evResult"

```



```
nitr0us@bukowski:~/android/com.markets.android$ sqlite3 --header "app_webview/Web Data" "select name|value|value_lower|date_created|date_last_used|count item_amount_1|100|100|1529451381|1529451381|1 cc_name_on_card|ALEJANDRO HERNANDEZ|alejandro hernandez|1529451381|1529451381|1 ni
```



ama

```
\Documents\cTrader\Journals\FxPro>type Journal-2018-07.txt
:43.493 | cTrader started
:54.572 | Demo account 10180548 successfully created
:11.993 | cTrader started
:42.160 | Limit order to Buy 0.1% 1k EURUSD (Price: 1.17203) is sent to server
:42.785 | 0.1% Limit order OID138943786 to Buy 0.1% 1k EURUSD (Price: 1.17203) is ACCEPTED (21/07/2018 23:29:42.395 UTC+0)
:02.160 | Limit order to Buy AUD 1k AUDSGD (Price: 1.01039) is sent to server
:02.394 | 0.1% Limit order OID138943787 to Buy AUD 1k AUDSGD (Price: 1.01039) is ACCEPTED (21/07/2018 23:30:02.294 UTC+0)
:48.306 | cTrader started
:20.431 | Limit order to Buy 0.1% 5k EURUSD (Price: 1.17203) is sent to server
:20.775 | 0.1% Limit order OID138943789 to Buy 0.1% 5k EURUSD (Price: 1.17203) is ACCEPTED (21/07/2018 23:47:20.578 UTC+0)
```

\Documents\cTrader\Journal Create Order - FxPro cTrader

FxPro
Trade Like a Pro

New Limit Order

Symbol: EURUSD, Euro vs US Dollar

Order Type: Buy Limit

Price: 1.17203
Volume: 5k €

Current distance: -0.1
Margin required: \$ 11.72

Order Entry

ISRG

462.92 463.26

BID MID ASK

BUY SELL

QTY 1,337 MKT MARKET DAY advanced

SUBMIT

Complete your Application

Ready to Start Trading?

Experience our best price execution and generate higher returns when you open and fund an actual account

Monitor Portfolio Favorites US Movers +

P&L + PROFILE

DAILY Unrealized 243.5K

Since prior Close

ISRG

Last Size 1

Last Exch 463.19

-7.84 -1.66%

Ask Exch

Bid Exch

Bid/Ask 462.92 x 463.26

Size 1 x 3

Hi/Lo 468.00 - 461.16

52 H/L 473.79 - 267.62

EARNINGS

EPS 9.40

P/E 49.3

ISRG 5 min candles

Alert Buy Sell

C:\Uts\dzgmivvzq\Thu.trd - Notepad++

Archivo Editar Buscar Vista Codificación Lenguaje Configuración Macro Ejecutar Plugins Ventana ?

Thu.audit.xml Thu.trd

5 35=8SOH34=000254SOH43=NSOH52=20180419-14:10:13SOH11=296181529.0SOH17=0001b25e.5
 d82a94.01.01SOH150=1SOH20=0SOH39=1SOH55=ISRGSOH100=AMEXSOH207=AMEXSOH38=1337SO
 44=0.00SOH32=100SOH30=AMEXSOH31=463.75SOH14=700SOH151=637SOH851=2SOH6=463.75SO
 54=1SOH37=002e9ace.00013e82.5ad81f72.0001SOH1=DU1010182SOH167=CSOH60=20180419-

```

098 D aTws : Keyboard up - don't show the submit slider
098 D aTws : Keyboard up - don't show the submit slider
098 D aTws : Keyboard up - don't show the submit slider
098 D aTws : Keyboard up - don't show the submit slider
15 I aTws : [OUT-01]: 8=FIX.4.109=0102035=d0320=86070094=76792991054=B01=DU7779180151=123
07228=1667831010=1210
15 I aTws : [IN-0-01]: 35=u06040=T0
15 I aTws : [IN-0-01]: 35=d0320=8607000=1011=95543343407228=166783107108=Filled0
15 I aTws : [OUT-01]: 8=FIX.4.109=m0320=8706040=S011=955433434010=1200
15 I aTws : [main]: hiding transmitSlider. set orderId=955433434
15 I aTws : [IN-0-01]: 35=m0320=87011=955433434072094=76792991055=TSLA014=B07219=TSLA072
01=DU77791807113=LIMIT07104=357.65014=12307108=Filled07110=DAY07115=#####07114=#00000000
0995=Bought 123 Limit 357.65 DAY06241=107270=00
15 E aTws : ERR [main]: Failed to update 'OE Profit Taken' Time-In-Force item since ''
supported=true;capabilities=0!,, GTC;supported=true;capabilities=0!,, OPG;supported=true;
15 E aTws : ERR [main]: Failed to update 'OE Stop Loss' Time-In-Force item since '' was
supported=true;capabilities=0!,, GTC;supported=true;capabilities=0!,, OPG;supported=true;orde
15 I aTws : [main]: hiding transmitSlider. checkOrderIsDone orderDone, Filled
15 I aTws : [main]: hiding transmitSlider since OrderStatus is done, y.a5be58af8f5
15 I aTws : [main]: hiding transmitSlider since OrderStatus is done, y.a5be58af8f5
15 I aTws : [main]: hiding transmitSlider since OrderStatus is done, y.a5be58af8f5
15 I aTws : [IN-0-01]: 35=u034=000012052=20170811-17:59:2606040=H0320=53850
15 I aTws : [OUT-01]: 8=FIX.4.109=0021035=u06040=h0320=5385010=1390
15 I aTws : [main]: ActivityState:(atws.activity.orders.OrderEditActivity@7fe215).finis
  
```

Buy Order

TSLA NASDAQ.NMS

357.87 +2.47 High 361.26

+0.69% Low 353.62

BID 5 x 357.70 357.99 x 1 ASK

DELAYED QUOTE

DU777918

Quantity 123

Time-in-force Day

Order type Limit

Limit price 357.65

Display size Show All

EUR/JPY

Market Order **Entry Order**

SELL BUY

Market: EUR/JPY

Units: 1,337

Rate: 131.567 ⓘ 0.0

Price PIPS

Take Profit: 132

Stop Loss

Trailing Stop

Lower Bound

Upper Bound

Units Available: 2,130,365
 1 PIP = 0.12 USD
 Take Profit: 5.12 USD / 43.3 PIPS
 Stop Loss: 0.00 USD / 0.0 PIPS
 Trade value: 1,556.88 USD
 Margin used: 62.28 USD

Keep open

```

239 2018-07-17 23:31:20.211 -0500 I [AWT-EventQueue-0] Buy/Sell window submitted
    : { } indicates disabled fields
240 [=== Market Order - EUR/JPY ===]
241 |Market Order|
242 ( ) SELL (o) BUY
243 Market [EUR/JPY]
244 Rate 131.564
245 (o) Price ( ) PIPS
246 [x] Take Profit
247 [ ] Stop Loss
248 [ ] Trailing Stop
249 { } Lower Bound
250 [ ] Upper Bound
251
252 Units Available: 2,130,498
253 1 PIP = 0.12 USD
254 Take Profit: 5.16 USD / 43.6 PIPS
255 Stop Loss: 0.00 USD / 0.0 PIPS
256 Trade value: 1,556.79 USD
257 Margin used: 62.27 USD
258 [ ] Keep open
259 2018-07-17 23:31:20.214 -0500 I [SwingWorker-pool-4298289-thread-10]
    Executing request: POST
    https://[REDACTED].com/v3/accounts/101-001-8050485-001/orders
    HTTP/1.1
260 2018-07-17 23:31:20.327 -0500 I [SwingWorker-pool-4298289-thread-10]
    response code: 201
261 2018-07-17 23:31:20.328 -0500 I [SwingWorker-pool-4298289-thread-10]
    response: {"orderCreateTransaction":{"type":"MARKET ORDER","instrument":
    "EUR_JPY","units":"1337","timeInForce":"FOK","positionFill":"DEFAULT",
    "takeProfitOnFill":{"price":"132.000","timeInForce":"GTC"},"reason":
    "CLIENT ORDER","id":"16","userID":"8050485","accountID":"101-001-8050485-001",
    "batchID":"16","requestID":"78482799175045436","time":
    "2018-07-18T04:31:19.609812908Z"},"orderFillTransaction":{"type":
    "ORDER_FILL","orderID":"16","instrument":"EUR_JPY","units":"1337","price":
    "131.564","pl":"0.0000","financing":"0.0000","commission":"0.0000",
    "accountBalance":"99999.9658","gainQuoteHomeConversionFactor":
  
```

SDJI 25013.29 +298.20 (+1.21%) SCOMPX 7394.04 +39.70 (+0.54%) CNAV 3733.01

C:\Users\nitr0us\AppData\Roaming\Charles Schwab\StreetSmart Edge\417756\Settings\settings.xml - No...

Archivo Editar Buscar Vista Codificación Lenguaje Configuración Macro Ejecutar Plugins Ventana ?

VendorTools.xml settings.xml exceptions.SSEdgeLog NCL.bt Screener.bt gics.bt PredefinedScreener

Watch List

My Positions TO INVEST LATER +

Add Symbol(s) Add Add Group

#	Symbol	News	Last T
4	NFLX		33
5	AMX		1
6	HACK		3
7	LOCO		1
8	AAPL		18
9	TSLA		28
10	PLNT		4
11	DOCU		4
12	ISRG		46

BA Go 363.92 ▲ +12.69 (3.5%)

Extended Hours: 364.15 ▲ +0.230 (0.06%)

BA : 20 Periods : 15 Minute +

Hide: Orders Positions

20 Periods : 15 Minute

11:00 12:00 13:00 14:00 15:00

Quick Jumps Date

```

p2:type="q2:guid">00000000-0000-0000-0000-000000000000
</anyType></value></item><item><key>IsExpanded</key><value><anyType
p2:type="q1:boolean">>false</anyType></value></item><item><key>EntryType
</key><value><anyType p2:type="q1:string">Symbol
</anyType></value></item></dictionary><dictionary><item><key>Name
</key><value><anyType p2:type="q1:string">PLNT
</anyType></value></item><item><key>Index</key><value><anyType p2:type=
"q1:int">9</anyType></value></item><item><key>Id</key><value><anyType
p2:type="q2:guid">00000000-0000-0000-0000-000000000000
</anyType></value></item><item><key>IsExpanded</key><value><anyType
p2:type="q1:boolean">>false</anyType></value></item><item><key>EntryType
</key><value><anyType p2:type="q1:string">Symbol
</anyType></value></item></dictionary><dictionary><item><key>Name
</key><value><anyType p2:type="q1:string">DOCU
</anyType></value></item><item><key>Index</key><value><anyType p2:type=
"q1:int">10</anyType></value></item><item><key>Id</key><value><anyType
p2:type="q2:guid">00000000-0000-0000-0000-000000000000
</anyType></value></item><item><key>IsExpanded</key><value><anyType
p2:type="q1:boolean">>false</anyType></value></item><item><key>EntryType
</key><value><anyType p2:type="q1:string">Symbol
</anyType></value></item></dictionary></dictionarylist></value></item><item
><key>Name</key><value><anyType p2:type="q1:string">TO INVEST LATER

```

length: 982692 lines: 43 Ln: 1 Col: 362147 Sel: 0 | 0 Dos\Windows UTF-8 INS



```
nitr0us@bukowski: ~/android/com.avatrade.mobile/shared_prefs
<map>
  <string name=".cached_watchlist.">EURUSD;;GBPUSD;;USDJPY;;AUDUSD;;USDCAD;;
  CrudeOIL;;GOLD;;BTCUSD;;ETH;;DJ30;;S&P500;;NASDAQ100;;DAX30;;#APPLE;;#GOOG
  LE;;USDMXN;;BTCEUR;;BTCJPY;;</string>
  <string name=".chart_state"><?xml version='1.0' encoding='UTF-8' standa
  lone='yes' ?&gt;&lt;bundle key=&quot;root&quot;&gt;&lt;string key=&quot;CHART_
  ID&quot; value=&quot;60147996&quot; /&gt;&lt;string key=&quot;edit_index&quot;
  value=&quot;-1&quot; /&gt;&lt;string key=&quot;show.tips&quot; value=&quot;tr
  ue&quot; /&gt;&lt;bundle key=&quot;0.parameters.bundle&quot;&gt;&lt;string key
  =&quot;parameters.count&quot; value=&quot;0&quot; /&gt;&lt;/bundle&gt;&lt;stri
  ng key=&quot;autoposition_mode&quot; value=&quot;true&quot; /&gt;&lt;string ke
  y=&quot;.fitVertical&quot; value=&quot>false&quot; /&gt;&lt;string key=&quot;.
  showPortfolio&quot; value=&quot>false&quot; /&gt;&lt;string key=&quot;show.ind
  icators&quot; value=&quot;true&quot; /&gt;&lt;string key=&quot;selected_instru
  ment&quot; value=&quot;#AT&amp;T&quot; /&gt;&lt;string key=&quot;0.fullnam
  e&quot; value=&quot;&quot; /&gt;&lt;string key=&quot;period&quot; value=&quot;
  DAY&quot; /&gt;&lt;string key=&quot;0.name.local&quot; value=&quot;&quot; /&gt;
  &lt;string key=&quot;.study_item_mode&quot; value=&quot;0&quot; /&gt;&lt;stri
  ng key=&quot;last_visible_candle&quot; value=&quot;2147483647&quot; /&gt;&lt;b
  undle key=&quot;.selectedStudy&quot;&gt;&lt;string key=&quot;size&quot; value=
  &quot;0&quot; /&gt;&lt;/bundle&gt;&lt;string key=&quot;show.legend&quot; value
  =&quot;true&quot; /&gt;&lt;string key=&quot;type&quot; value=&quot;1&quot; /&g
  t;&lt;string key=&quot;range&quot; value=&quot;YEAR1&quot; /&gt;&lt;string key
  =&quot;0.fullname.local&quot; value=&quot;&quot; /&gt;&lt;string key=&quot;aut
  oscale_mode&quot; value=&quot;true&quot; /&gt;&lt;string key=&quot;0.enabled&
  uot; value=&quot;true&quot; /&gt;&lt;string key=&quot;compact&quot; value=&quo
  t;false&quot; /&gt;&lt;string key=&quot;0.name&quot; value=&quot;&quot; /&gt;&
  lt;bundle key=&quot;0.plots.bundle&quot;&gt;&lt;string key=&quot;plots.count&
  uot; value=&quot;0&quot; /&gt;&lt;/bundle&gt;&lt;string key=&quot;data_state&
  uot; value=&quot;2&quot; /&gt;&lt;string key=&quot;candleWidth&quot; value=&qu
  ot;1&quot; /&gt;&lt;/bundle&gt;</string>
```

```
I System.out: <WatchList>
I System.out: <WatchListId>1268844001</WatchListId>
I System.out: <WatchListTune>0</WatchListTune>
I System.out: <WatchListName>POTENTIAL INVESTMENTS</WatchListName>
I System.out: </WatchList>
I System.out: </GetWatchListsResponse>
I ActivityManager: Displayed com.etrade.mobilepro.activity.com

I System.out: Before calling service url /e/t/mobile/GetWatchListEntriesResponse
I System.out: response is <GetWatchListEntriesResponse xmlns:="http://www.etrade.com/et/mobile/GetWatchListEntriesResponse.xsd" servicename="mobile">
I System.out: <Result code="0">
I System.out: <Fault/>
I System.out: </Result>
I System.out: <WatchListId>1268844001</WatchListId>
I System.out: <Product>
I System.out: <Symbol>CIBR</Symbol>
I System.out: <Display_Symbol>CIBR</Display_Symbol>
I System.out: <TypeCode>EQ</TypeCode>
I System.out: <ExchangeCode>NSDQ</ExchangeCode>
I System.out: <EntryId>3344135001</EntryId>
I System.out: <ExchangeGroup>US</ExchangeGroup>
I System.out: <DateAcquired>07/29/2017</DateAcquired>
I System.out: </Product>
I System.out: <Product>
I System.out: <Symbol>AAPL</Symbol>
I System.out: <Display_Symbol>AAPL</Display_Symbol>
I System.out: <TypeCode>EQ</TypeCode>
I System.out: <ExchangeCode>NSDQ</ExchangeCode>
I System.out: <EntryId>3344137001</EntryId>
I System.out: <ExchangeGroup>US</ExchangeGroup>
I System.out: <DateAcquired>07/25/2017</DateAcquired>
I System.out: </Product>
I System.out: <Product>
I System.out: <Symbol>SPY</Symbol>
I System.out: <Display_Symbol>SPY</Display_Symbol>
```

Symbol	Last	Change \$	Change %	Volume
CIBR	21.1699	-\$0.25	-1.14%	69
AAPL	157.02	\$6.97	4.65%	54
SPY	246.975	-\$0.34	-0.14%	25
NTDOY	42.35	\$0.29	0.68%	374
HACK	29.08	-\$0.39	-1.32%	277
TSLA	323.60	\$4.03	1.26%	5
NTDOY	42.35	\$0.29	0.68%	374

```
nitr0us@bukowski:~/android/com.firsttrade.android$ strings app
Cache/99c50ebdbfed13b7_0 | grep symbol
t$https://api3x.firsttrade.com/private/getfav{"statusCode":200
e:"Normal","result":{"list_id":1,"name":"Mobile Favorites","
hlist_id":1186971,"sec_type":1,"symbol":"B","quantity":0,"las
ask":60.01,"vol":285947,"change":1.32,"change_percent":2.26,"
"unit_cost":0,"cost":0,"gain_amount":0,"gain_percent":0,"bid
"high":60.24,"low":59.31,"close_price":58.68,"update_time":0
hlist_id":1186905,"sec_type":1,"symbol":"EWW","quantity":0,"l
.68,"ask":56.69,"vol":1147548,"change":0.67,"change_percent":
nt":0,"unit_cost":0,"cost":0,"gain_amount":0,"gain_percent":0
ize":14,"high":56.89,"low":56.41,"close_price":56.01,"update
},{ "watchlist_id":1186914,"sec_type":1,"symbol":"GRBMF" "quan
,"bid":2.45,"ask":2.49,"vol":1800,"change":0.06,"change_perce
amount":0,"unit_cost":0,"cost":0,"gain_amount":0,"gain_perce
"asksize":100,"high":2.5,"low":2.48,"close_price":2.42,"updat
m"}, {"watchlist_id":1186926,"sec_type":1,"symbol":"SPY","quan
6,"bid":246.6,"ask":246.61,"vol":51302492,"change":2.47,"chan
```

Symbol	Last	Change	Volume
B	60.00	+1.32	289.6K
EWW	56.68	+0.67	1.2M
GRBMF	2.48	+0.06	1.8K
SPY	246.67	+2.54	53.3M

```
[OUT-0]: 8=FIX.4.109=0060035=w0320=5207027=007094=15824958207131=2h09920
[IN-0-01]: 35=w06119=520320=52055=GXPR058=GOPRO INC-CLASS A@127=10007116
64/1;964/2;964/3;962/4;962/5;964/6;965/7;964/8;965/9;964/10;964/11;965/12
965/21;964/22;966/23;966/24;966/25;966/26;968/27;967/28;968/29;967/30;969
89;970/40;970/41;971/42;971/43;971/44;971/45;972/46;970/47;972/48;971/49;
96/58;975/59;975/60;975/61;975/62;976/63;976/64;975/65;975/66;975/67;975/
6;981/77;981/78;981/79;983/80;983/81;983/82;982/83;982/84;982/85;980/86;9
2/95;979/96;979/97;979/98;981/99;980/100;979/101;980/102;980/103;979/104;
0007213=107214=207233=20
[IN-0-01]: 35=w ChartData 38375662 : Can pan back: true ticks:106 max:150
[IN-0-01]: 35=w TimeSeriesManager: Server id set:52
[OUT-01]: 8=FIX.4.109=0085035=I0320=5301=DU77791807094=15824958206119=Q16
[ WorkerThread]: 35=w TimeSeriesManager: processor removed unsubscribe T
ey[key=158249582:2h::%c/%t:-:fx_p_off], m_serverId=52, m_reqId=52] total
[ WorkerThread]: 35=w TimeSeriesManager: Clear
[OUT-01]: 8=FIX.4.109=0012035=w0320=54010=1770
requesting -1 chart bars; isPan=false; TimeSeriesKey[key=6257:2h::%c/%t:
[ WorkerThread]: 35=w TimeSeriesManager: setKeyData reqId:55 key:TimeSer
[OUT-01]: 8=FIX.4.109=0080035=I0320=5601=DU77791807094=625706119=Q1707091
[ WorkerThread]: 35=w TimeSeriesManager: Added processor for TimeSeriesF
?2h::%c/%t:-:fx_p_off], m_serverId=null, m_reqId=55]
[OUT-01]: 8=FIX.4.109=0055035=w0320=5507027=007094=625707131=2h09920=1001
[ WorkerThread]: 35=w TimeSeriesManager: Subscribe response processors c
[IN-0-01]: 35=w06119=550320=55055=CX058=CEMEX SAB-SPONS ADR PART CER07127
9=925/0;925/1;925/2;924/3;924/4;924/5;924/6;924/7;924/8;925/9;926/10;926/
9;926/20;926/21;927/22;927/23;926/24;926/25;926/26;927/27;927/28;927/29;9
```

INSTRUMENT	LAST	CHG	%CHG	VOL
GPRO NASDAQ:NMBS	9.78	0.00	0.00%	2.52M
CX NYSE	9.24	-0.05	-0.54%	4.55M

2h

9.28 TODAY 9.37 High
9.27 9.23 Low
9.26 52WK High
Low
9.25 Bid 9.24 x 454
9.24 Ask 9.25 x 689

ADD INSTRUMENT


```

Expected exception: java.io.WriteAbortedException: writing aborted
    call determinedVisibility() - never saw a connection for the pic
javascript_dialog_manager.cc(68)] Not implemented reached in virt
ndingDialogs(content::WebContents*)
    call determinedVisibility() - never saw a connection for the pic
javascript_dialog_manager.cc(68)] Not implemented reached in virt
ndingDialogs(content::WebContents*)
)l "Failed to decode downloaded font: file:///android_asset/www/s
le:///android_asset/www/src/charts/index.html?symbol=EWW (0)
)l "OTS parsing error: invalid version tag", source: file:///and

)l "Failed to decode downloaded font: file:///android_asset/www/s
e:///android_asset/www/src/charts/index.html?symbol=EWW (0)
)l "OTS parsing error: invalid version tag", source: file:///and

Expected exception: java.io.WriteAbortedException: writing aborted
Expected exception: java.io.WriteAbortedException: writing aborted
Expected exception: java.io.WriteAbortedException: writing aborted
tofill_client.cc(121)] Not implemented reached in virtual void x
tofill_client.cc(121)] Not implemented reached in virtual void x

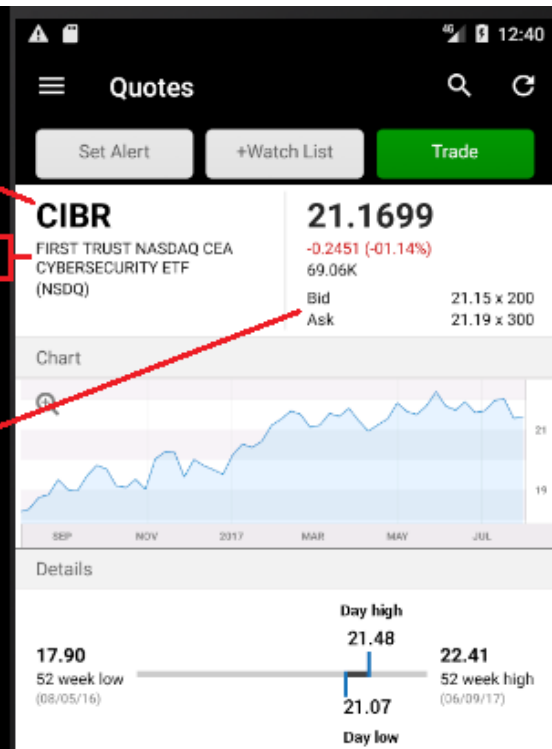
```



```

I System.out: <Quote>
I System.out: <Symbol>CIBR</Symbol>
I System.out: <ProductType>EQ</ProductType>
I System.out: <ExchangeCode>NSDQ</ExchangeCode>
I System.out: <ExchangeName>NASDAQ NM</ExchangeName>
I System.out: <ExchangeDesc/>
I System.out: <TypeName>Equity</TypeName>
I System.out: <TypeDesc/>
I System.out: <Currency>USD</Currency>
I System.out: <ProdStatus>1</ProdStatus>
I System.out: <ProdSvcRetnStatus>0</ProdSvcRetnStatus>
I System.out: <SymbolDesc>FIRST TRUST NASDAQ CEA CYBERSECURITY
I System.out: <Low>21.07</Low>
I System.out: <FastMktFlag>0</FastMktFlag>
I System.out: <NextEarningsDate>0/0/0</NextEarningsDate>
I System.out: <AskSize>200</AskSize>
I System.out: <Price>21.1699</Price>
I System.out: <BidSize>200</BidSize>
I System.out: <QuoteType>Real Time</QuoteType>
I System.out: <IsDecimalFlag>True </IsDecimalFlag>
I System.out: <QuoteStatus>0</QuoteStatus>
I System.out: <NewsFlag>False </NewsFlag>
I System.out: <Close>21.415</Close>
I System.out: <Hi>21.48</Hi>
I System.out: <TimeZone>EST</TimeZone>
I System.out: <Ask>21.19</Ask>
I System.out: <Volume>67,012</Volume>
I System.out: <Open>21.48</Open>
I System.out: <Bid>21.15</Bid>
I System.out: <QuoteExchangeCode>NSDQ</QuoteExchangeCode>
I System.out: <QuoteSymbol>CIBR</QuoteSymbol>
I System.out: <TimeStamp>08/02/17-1:31:00PM ET</TimeStamp>
I System.out: <HaltedFlag>0</HaltedFlag>
I System.out: <Change>-0.25</Change>

```



- Some brokers such as **Plus500** or **MetaTrader** allow their customers to choose easily guessable passwords

eguro | <https://www.mql5.com/en/users/bukowski31337/security>

Change password

New password: Confirm:
Password must exceed 4 characters Password must exceed 4 characters

Confirm your authorization to apply changes

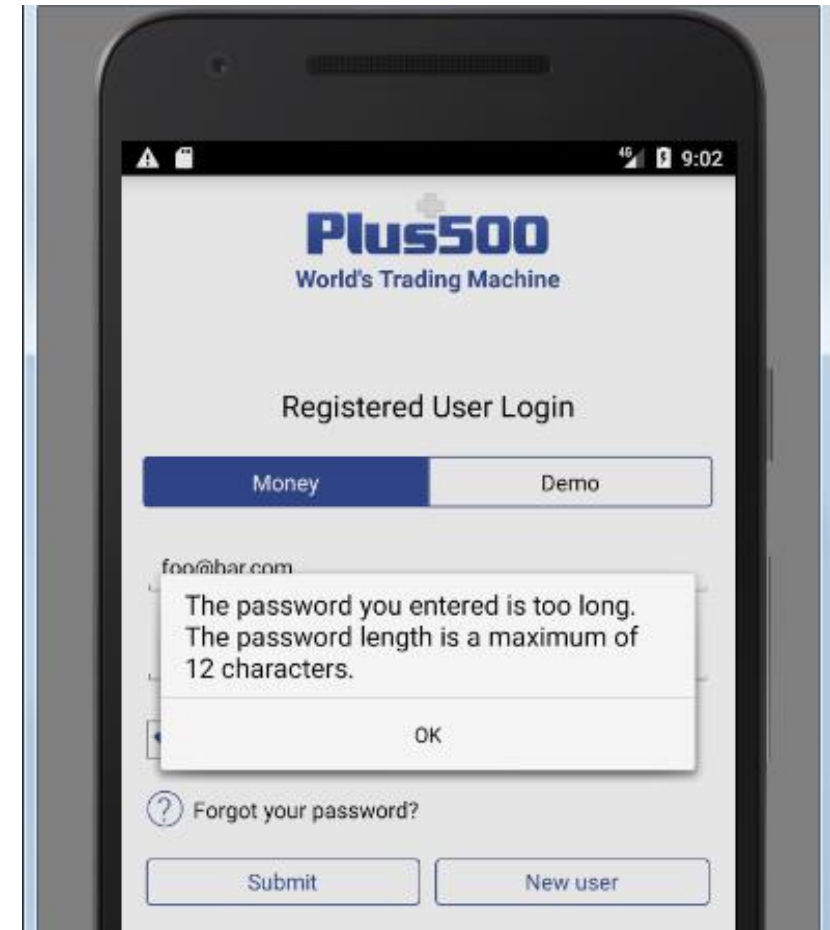
Current password: **12345**

MQL5 WebTerminal Documentation C

bukowski31337

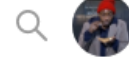
Profile Settings

Successfully saved



- Some brokers such as **IQ Option** and **Markets.com** validate the password policy client-side only





Change Password

If you notice any suspicious activity, we recommend changing your password.

Any questions about how to set up personal data?

Visit our [Help Center](#)

Enter your old password

Enter a new password

Cancel Save

Password Strength: Your password must be at least 6 characters long and contain at least 1 letter and 1 number

Average

Session History

Information about the use of your account. Last activity: today at 9:51 pm (Browser Chrome)

Request

Raw Params Headers Hex

```
POST /api/profile/password HTTP/1.1
Host: iqoption.com
Connection: close
Content-Length: 362
Origin: https://iqoption.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLNcErL0P16Hx0soS
Accept: */*
Referer: https://iqoption.com/en/profile/security
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8
Cookie: _ga=GAL.2.980530117.1522723886; _gid=GAL.2.1599770701.1522723886; landing=iqoption.com; red_test_ab={%22random_id%22:%22F832FD49-F1C7-B462-455D-A4C747D8EC62%22%2C%22group%22:1}; _uetid=uet94f963e7; _ym_uid=1522723892832780991; lang=en_US; pll_language=en; _ym_isad=2; _ym_visorc_22669009=w; ssid=f763c78d630alaf9d94821cd83431772; _uat=c9c64e071d2853bc7906c017a231ad1cc46ab630; platform=15; is_regulated=0

-----WebKitFormBoundaryLNcErL0P16Hx0soS
Content-Disposition: form-data; name="current_password"

Qwertyf00b4r
-----WebKitFormBoundaryLNcErL0P16Hx0soS
Content-Disposition: form-data; name="password"

123456
-----WebKitFormBoundaryLNcErL0P16Hx0soS
```

Response

Raw Headers Hex JSON Decoder

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 03 Apr 2018 02:56:46 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
Set-Cookie: _uat=c9c64e071d2853bc7906c017a231ad1cc46ab630; path=/
Set-Cookie: ssid=69938bd98d5db64728c9e7e0eca2acc1; expires=Thu, 03-May-2018 02:56:46 GMT; Max-Age=2592000; path=/; domain=iqoption.com
Set-Cookie: ssid=69938bd98d5db64728c9e7e0eca2acc1; expires=Thu, 03-May-2018 02:56:46 GMT; Max-Age=2592000; path=/; domain=iqoption.com
Set-Cookie: ssid=69938bd98d5db64728c9e7e0eca2acc1; expires=Thu, 03-May-2018 02:56:46 GMT; Max-Age=2592000; path=/; domain=iqoption.com
X-Front-Host: fe-api-03
Access-Control-Allow-Origin: https://iqoption.com
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Strict-Transport-Security: max-age=15555600
X-Content-Type-Options: nosniff
Content-Length: 88

{"isSuccessful":true,"message":["Your password was successfully changed"],"result":null}
```

SETTINGS



Customer Info

Leverage Settings

Change Password

Notifications

Platform Features

Change your password

Current password

New password

Retype password

Your password must contain 6-15 characters (digits and letters only), with at least one number, one lowercase letter and uppercase letter.

Edited request

Response

Headers

Hex

```
g6092921_24.group24=S1529523710.a4d2da75b7; lc_window_state.group24=minimized; incap_ses_978_756=VTExoJqVS3m5fbubBlrrYrGGuK1sAAAAAQUIPAAAAABpfj9e5r/sfcWfcIIRFWsz; incap_ses_979_1087756=EBFCZMNGNUQIDV%3A20180620%3A9%7CBZVJR4NSSBABPMPXBZNV7H%3A20180620%3A9%7C7EGFWRP2BZBEH3ZKXFBEBJg6092921_27.group27=S1529523815.900924e9af; visid_incap_1204500=fyy9YfbsSNCghflfQSP36CquK1sAAYN1MZWgaQbd3gWHBEjwAAAADtuHqBXf9acZeis47pww05; incap_ses_978_1204500=PMX9exh5jkrSGwaS4J46SDWqu
```

```
hashedPassword=60b49a6caefec54a3e9661b1145fa476&oldPassword=Qwertyf00b4r&newPassword=123
```

Original request

Edited request

Response

Raw

Headers

Hex

JSON Decoder

```
{
  "body": "ff2fd59f913d8b8632bbb9707581be54",
  "success": true
}
```

Save Changes

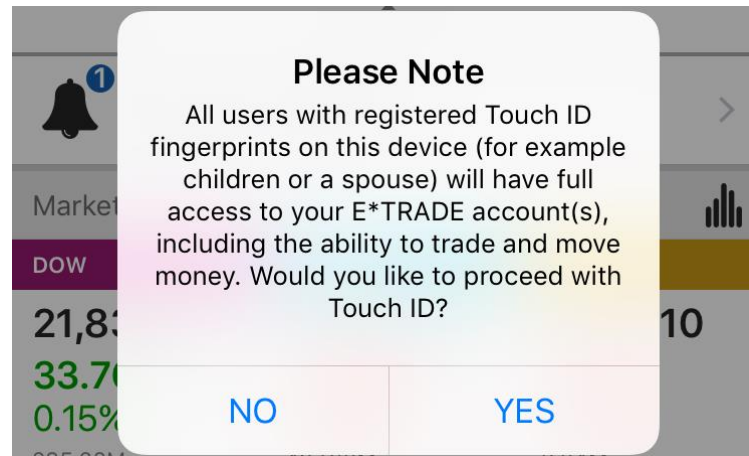
✓ Changes saved

Used Margin: \$0.00

Real Account

Profit / Loss \$0.00

- Most **web**-based trading platforms **implement 2FA**
- Most **desktop** platforms **do not implement 2FA**
 - Even from same broker
- 8 mobile apps (24%) do not implement **fingerprint** auth
 - Downside:



- Session tokens passed through the URL are Single Sign-on (SSO)
 - Usable once
 - A race on who opens the URL first
- Attacker or malware could leave an endless loop sensing the OS process list
 - Unlikely but feasible
 - One second is enough to hijack a session

USD/CAD Option AUD/JPY Option AUD/CAD Forex EUR/CAD Forex CAD/CHF Forex Bitcoin +64.72%

PRACTICE ACCOUNT \$ Deposit

TOTAL PORTFOLIO ACTIVE PENDING

John Spencer Change Photo Personal Data

Mexico Deposit Withdraw Funds OTN Tokens Contact Support Transactions History Trading History

15 Aug 2017 Date registered

5:42 Profit @ 50% 668.50

```
245:1|248:1|253:0|254:0|255:0|256:1|257:1|258:0|259:1|264:0|267:1|268:1|269:1|270:1|271:1|272:0|273:0|279:1|282:0|283:0|284:1|285:1|286:0|287:1|288:1|289:0|492307:0|306:0|305:0|304:1|303:1| -stringPrefs 3:7;release|151:0|212:3;1.0|223:332; ...
New Process: "/usr/lib/firefox/firefox https://auth.iqoption.com/api/v1.0/login/token?q=MjE1MTk2NTh8MzFlNjY2NjhhYmZmNWl2ZWJmMTcxZjlmNThiMzNkMTJhZjcxMDE4MjE0OGYyMGFhY2I2NzlkZjExMTYzZWESMDE1ZGI0YzgzMGZiYzE2MThjNTEyNjNhODMzYTQ1MjRlMWNjY2M2YWRlMzY4NmRiYWJmMmM4YTh8AHR0cHM6Ly9pcW9wdGlvbi5jb206NDQzL3Byb2ZpbGU%3D"
New Process: "/usr/lib/x86_64-linux-gnu/indicator-messages/indicator-messages-service"
New Process: "/sbin/agetty --noclear tty2 linux"
New Process: "/usr/lib/NetworkManager/nm-dispatcher"
```

Personal Data

Es seguro | https://iqoption.com/en/profile/personal

iq option® Ultimate trading experience

Deposit Trade Now

Personal Data Wallet Withdraw Funds

John Spencer Delete photo Change

DOWNLOAD for Windows .exe 15.9 Mb


```
cmd.exe "C:\Windows\system32\cmd.exe" /D /C C:\Users\nitr0us\AppData\Local\Temp\i4j2705805036353281235.bat
  tws.exe "C:\Jts\tws.exe" -J-DskipUpdateCheck=true
    firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -osint -url "https://gdcdyn.interactivebrokers.com/sso/AuthenticateTWS;JSESSIONID=4D896706074D7904D93B6007C584B26C.www.sso1?acct_id=DU1010182&action=ACCT_MGMT..."
      firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="6788.0.974915320\1841696634" -greomni "C:\Program Files (x86)\Mozilla Firefox\omni.ja" -appomni "C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja" -app
      firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="6788.0.126102888\1863437155" -childID 1 -isForBrowser -intPrefs 6:50|7:-1|34:1000|42:20|43:5|44:10|51:0|57:128|58:10000|63:0|65:400|66:1|67:0|68:0|69:100|74:
      firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="6788.0.13.2101103374\2132283382" -childID 2 -isForBrowser -intPrefs 6:50|7:-1|34:1000|42:20|43:5|44:10|51:0|57:128|58:10000|63:0|65:400|66:1|67:0|68:0|69:100|74:
      firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="6788.0.20.260619321\1885287538" -childID 3 -isForBrowser -intPrefs 6:50|7:-1|34:1000|42:20|43:5|44:10|51:0|57:128|58:10000|63:0|65:400|66:1|67:0|68:0|69:100|74:
```

Account Management x Activity Statement May 1 x

Interactive Brokers LLC [US] | https://gdcdyn.interactivebrokers.com/Universal/servlet/AccountAccess.AuthenticateSSO?action=ACCT_MGMT_MAIN&clt=1&mid=001

Trade Reports Manage Account Support Logout

- Activity >
- Trade Confirmations
- Tax

- Statements
- Flex Queries
- Models
- Batch Reports

Not Available

Current Margin Requirements (USD)

May 21, 2018 12:00 PM EDT

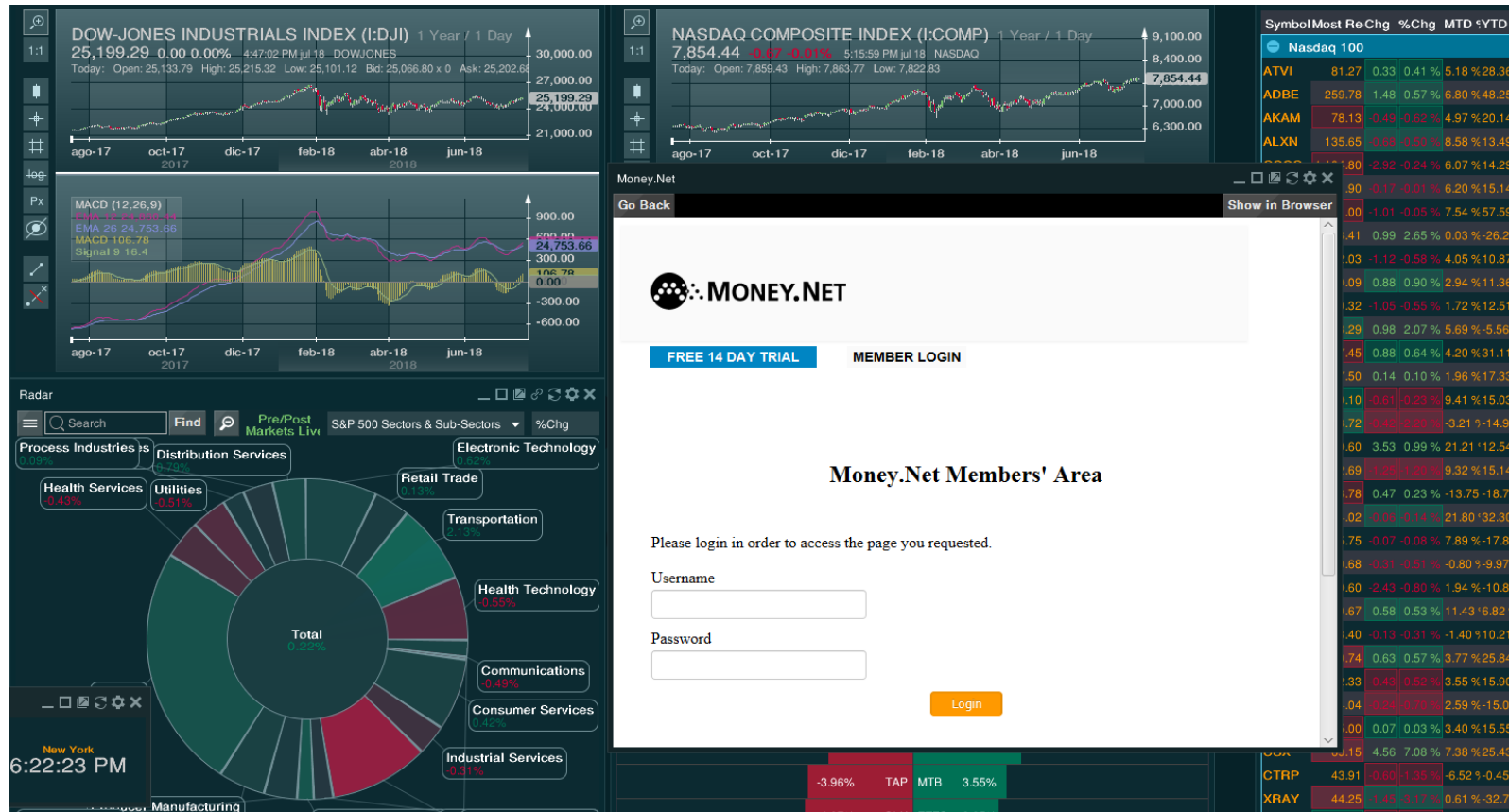
IB offers a comprehensive program of professional trader webinars that can be viewed live or played back at any time from your computer.

[View entire list of webinars.](#)

DEMO

Charles Schwab
URL session hijacking. URLs
with SSO tokens passed as
parameters to the browser.
Could be stolen from the
process list.

- Platforms such as **Money.Net** implement their own Web UI
- Also allow the user to use it or use the default web browser



The screenshot displays a financial dashboard with several components:

- Top Left:** DOW-JONES INDUSTRIALS INDEX (I:DJI) chart showing a price of 25,199.29.
- Top Middle:** NASDAQ COMPOSITE INDEX (I:COMP) chart showing a price of 7,854.44.
- Top Right:** Table of Nasdaq 100 stocks with columns for Symbol, Most Re, Chg, %Chg, MTD, and %YTD.
- Bottom Left:** Radar chart showing S&P 500 Sectors & Sub-Sectors with various categories like Process Industries, Distribution Services, etc.
- Bottom Center:** Money.Net Members' Area login form with fields for Username and Password, and a Login button.
- Bottom Right:** Additional stock data for CTRP and XRAY.

- Clicked on the “logout” button
- Sent a previously captured request **+1 hour later**
- Worked!
 - **E-TRADE**
 - **Charles Schwab**
 - **Fidelity**
- Session should be destroyed in both sides, server and client



Logged off

i You have been logged off your E*TRADE account. To start a new session, simply log on when you're ready.

buk*****

.....

Remember my user ID

[Forgot your User ID or Password?](#)



Don't have an E*TRADE account?
[Start investing now](#)

Did
Set

Response

Raw Headers Hex HTML Render

[Last refresh](#) March 02, 2018 5:19 PM ET

Balances

Account: Individual Brokerage -2213

GO

[+ Show](#)

[Refresh](#)

Previous Close

Real-Time Values
as of 03/02/18 5:19 PM ET

Net Account Value

\$0.00

Total Market Value of Securities

\$0.00

Cash Available for Investment

\$0.00

Cash Available for Withdrawal

\$0.00

Net Cash Balance **i**

\$0.00

[+ Show Detailed Balances](#)



Logged off

You have been logged off your E*TRADE account. To start a new session, simply log on when you're ready.

buk*****

.....

Response Raw Headers Hex JSON Decoder

```
"data": {
  "lastRefreshDate": "03/02/18 05:04 PM ET",
  "portfolioAccountValues": {
    "unsettledCash": 0,
    "intradayMarginableSecurities": 0,
    "intradayMrgnPurPowerBeforeOrderReserve": 0,
    "overnightNonMrgnReserveForOpenOrders": 0,
    "nonMrgnReserveForOpenOrders": 0,
    "availableForWithdrawalVal": 0,
    "totalGainVal": 0,
    "excessEquityPurPowerBeforeOrderReserve": 0,
    "isAllBrkrgrAccntRequest": 0,
    "settledCash": 0,
    "overnightMrgnReserveForOpenOrders": 0,
    "isManagedAccount": null,
    "nonMrgnPurPowerAfterOrderReserve": 0,
    "cashAvlForWithdrawal": 0,
    "daysGainRealizedVal": 0,
    "cashPurchasingPower": 0,
    "contributionsPrevYear": 0,
    "intradayMrgnPurPowerAfterOrderReserve": 0,
    "overnightNonMrgnPurPowerBeforeOrderReserve": 0,
    "mrgnPurPowerBeforeOrderReserve": 0,
```

```
"isMargin": false,
"role": "PRI",
"accountShortName": "Individual Brokerage ██████",
"futuresEligible": false,
"accountName": "",
"dtStatusCd": "1",
"marginLevelCd": "1",
"accountDesc": "Individual Brokerage",
"accountType": "INDIVIDUAL",
"optionLevelCd": "2",
"institutionType": "ADP",
"tcpEligible": "2",
"accountNumber": "██████",
"institutionNo": "██████",
"benfPermission": "2",
"accountKey": "go7jL2mKKe4qKIH4Bai9V1TVVg0a0jdfTqTNoFJsI",
"futuresInProgress": false,
"typeIRA": false,
```

User ID

or Password?

Log on

Log Out Successful

You are now logged off. Thank you for using Charles Schwab.

Log In

Request

Raw Headers Hex

```
GET /api/customerAccount.MyProfile/v1/HeaderInformation HTTP/1.1
Host: jfkgateway.schwab.com
Connection: close
Schwab-CorrelationId: bc8f88fe-8b35-4c34-9829-flf3f84135a6
Origin: https://client.schwab.com
Authorization: Bearer
IO.b2FldGgyLmJkYy5zY2h3YWluY29t.-9CjwWmoFTPqjzZzlu290dWNAEUn3dtgaLEvTTF2ZzQ@
Schwab-ChannelCode: IO
Accept: application/json
Schwab-Env: DEFAULT
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
Schwab-Gateway-Scope: api
Referer: https://client.schwab.com/Apps/service/myprofile/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8
```

Response

Raw Headers Hex JSON Decoder

```
{
  "LoginId": "██████████",
  "QuerySuccessful": false,
  "Parties": [
    {
      "TaxPayerId": "██████████",
      "CountryOfResidence": "US",
      "DateOfBirth": "██████████-05",
      "CustTypeCd": "IND",
      "OrgTypeCd": "",
      "FirstName": "JOHN",
      "OtherName": "",
      "SuffixName": "",
      "OrgName": "",
      "MiddleName": "",
      "Citizenships": [
        {
          "CountryOfCitizenship": "US"
        }
      ]
    }
  ]
}
```

SCHWAB PERSONAL TRUST SERVICES

Looking to name a corporate trustee?



Learn more about professional trust management >

Log Out Successful

You are now logged off. Thank you for using Charles Schwab.

Log In

SCHWAB PERSONAL TRUST
SERVICES

Looking to name a
corporate trustee?

Request

Raw Params Headers Hex

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://client.schwab.com/Areas/Accounts/Balances
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8
Cookie: lms-lang=en-US; aam_uuid=37759553817204013323956494583874839040; lang=en-US; check=true; bm_mi=4911C4A04EFCDE633642879217415535D~uwMVm2xoM4tHM5gwV4cGZxCzxFjaC52x7IGrt1QLKcz229BIZCVnIc6RCaIDBwS5cqvBhKJT03GpfrctzyE/a5830q5vmfw0iNVc6U+ioc5mte8rBHmtRYUMVoDMNd7KACJ28GKeuT2/X4vA/D8ErrxPCqvt8L4QcJTtVWILpwN+MWWJkbgXn4XoqfrxH7mTZM+pegtJwQ9ySzitssAaJyuXCoxkRhx3eLIXZ6d+DfmPB2AUjMEQw8jXU4AQWudN0mFRA97embHL4V840cDScLGzw==; mbox=session#d790fff226e94e31815e9ff8a411acad#1523421549|PC#d790fff226e94e31815e9ff8a411acad.28_68#1586664065; ak_bmsc=B9CD8DC72D4E812499BAB5D58E9E2CC642ABE160232E00007B88CD5A2421D936~p1BDlseRDgZRMWzp+nimizoR20vL71VN+AT7b4tm09t0h02sgULpFSYUAf6By9yA0p/MND81m7Si+RiX2XGNEyKY78RegB1aUS3RkbbJzpg0XymXbVUySVKph3T1deIe4yUkge1AeU7Vr3isn52KW811HvK9yptPNWv2UU4aGWBnxLeCC1UA01iH5NChP9Bs7Tt9di+y0RlpZo33FebJFyp6GVMcDZgym26Yh/zSgqxvTy913g0DAcVPj8Mr9481v; AMCVS_SDB5123F5245B1D20A490D45440AdobeOrg=1; s_vi=[CS]v1|2D66C514051D01C3-4000191100001AF6[CE]; lms-dynamic-cookie=startin=CCBodyi&cpn=N; ADRUM=s=1523419746878&r=https%3A%2F%2Fms.schwab.com%2FLogin%3F-1960276895; BIGipServerclient-origin-rr-bdc-443-pool=403203850.47873.0000; aam_uuid=37759553817204013323956494583874839040;
```

Response

Raw Headers Hex HTML Render

Total Cash & Cash Investments

\$0.00

Total Market Value

\$0.00

Day Change **

\$0.00 (0%)

Brokerage Accounts

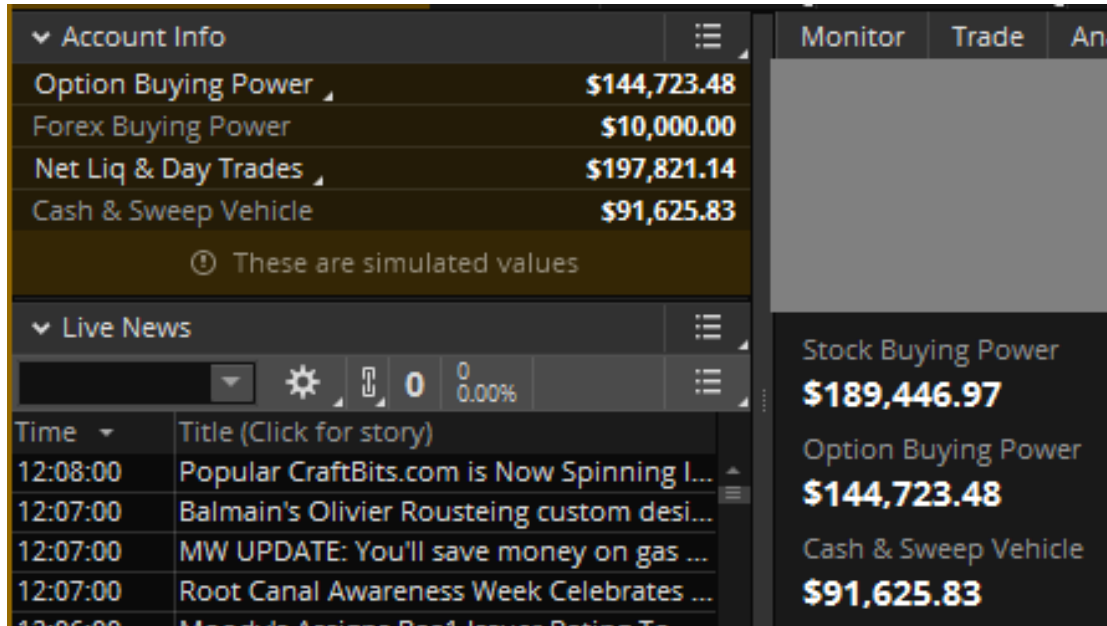
Name	Account	Cash & Cash Investments	Account Value	Day Change **
Individual	9664-7547	\$0.00	\$0.00	+\$0.00 (0%)
Totals		\$0.00	\$0.00	+\$0.00 (0%)

- Protects private information from being displayed on the screen in public areas where **shoulder-surfing** attacks are feasible
 - Most platforms do not implement this feature





- TD Ameritrade's Thinkorswim for desktop
 - Before and after enabling the privacy mode



Account Info

Option Buying Power	\$144,723.48
Forex Buying Power	\$10,000.00
Net Liq & Day Trades	\$197,821.14
Cash & Sweep Vehicle	\$91,625.83

These are simulated values

Live News

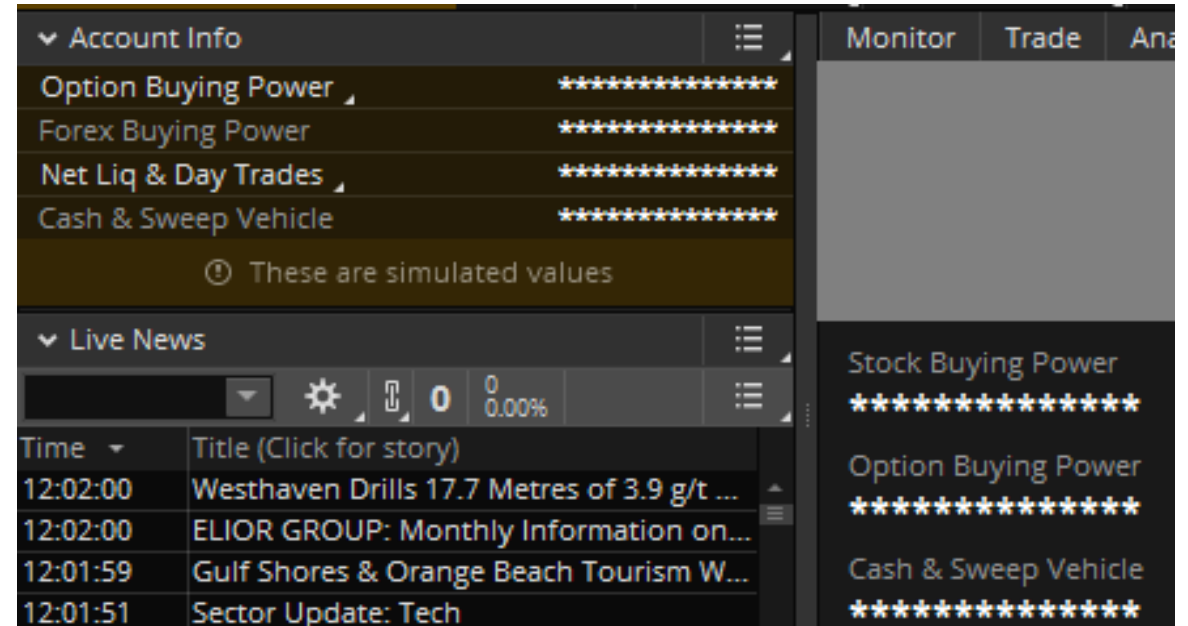
Time	Title (Click for story)
12:08:00	Popular CraftBits.com is Now Spinning I...
12:07:00	Balmain's Olivier Rousteing custom desi...
12:07:00	MW UPDATE: You'll save money on gas ...
12:07:00	Root Canal Awareness Week Celebrates ...
12:06:00	Market Update: Real Estate Rating To...

Monitor Trade Ana

Stock Buying Power
\$189,446.97

Option Buying Power
\$144,723.48

Cash & Sweep Vehicle
\$91,625.83



Account Info

Option Buying Power	*****
Forex Buying Power	*****
Net Liq & Day Trades	*****
Cash & Sweep Vehicle	*****

These are simulated values

Live News

Time	Title (Click for story)
12:02:00	Westhaven Drills 17.7 Metres of 3.9 g/t ...
12:02:00	ELIOR GROUP: Monthly Information on...
12:01:59	Gulf Shores & Orange Beach Tourism W...
12:01:51	Sector Update: Tech

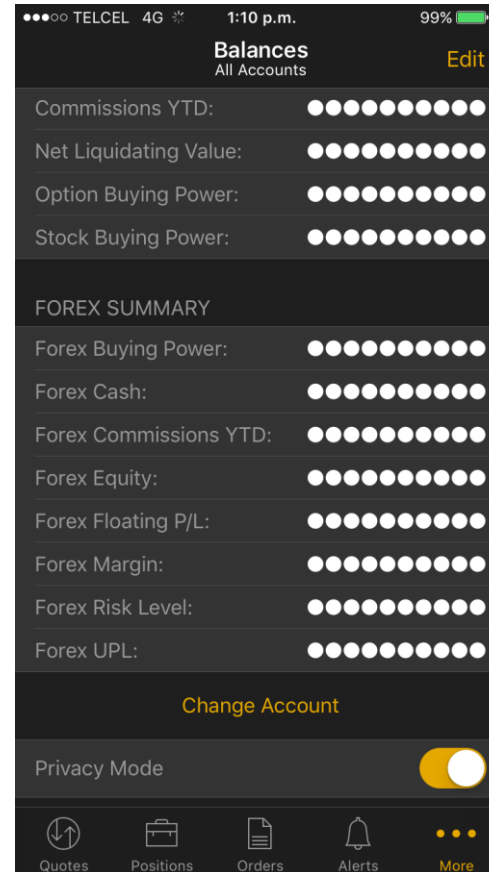
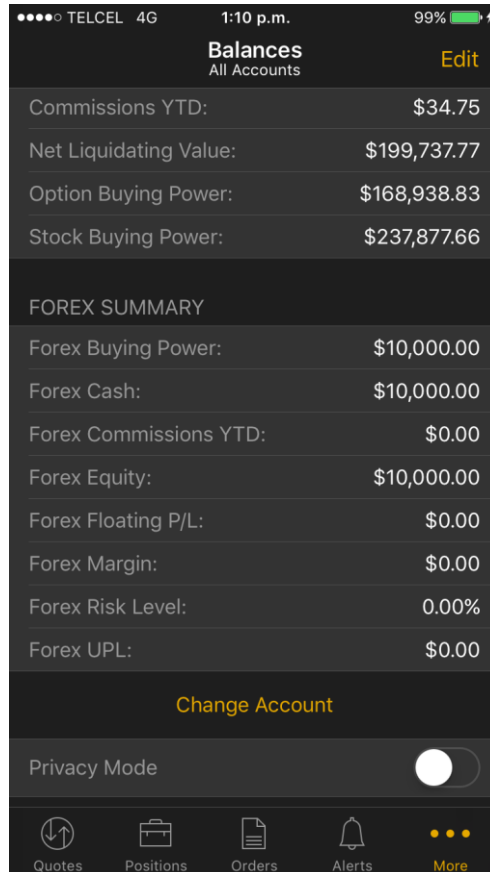
Monitor Trade Ana

Stock Buying Power

Option Buying Power

Cash & Sweep Vehicle

- **TD Ameritrade's Thinkorswim for mobile**
 - Before and after enabling the privacy mode



- **Yahoo! Finance**
 - After enabling the privacy mode

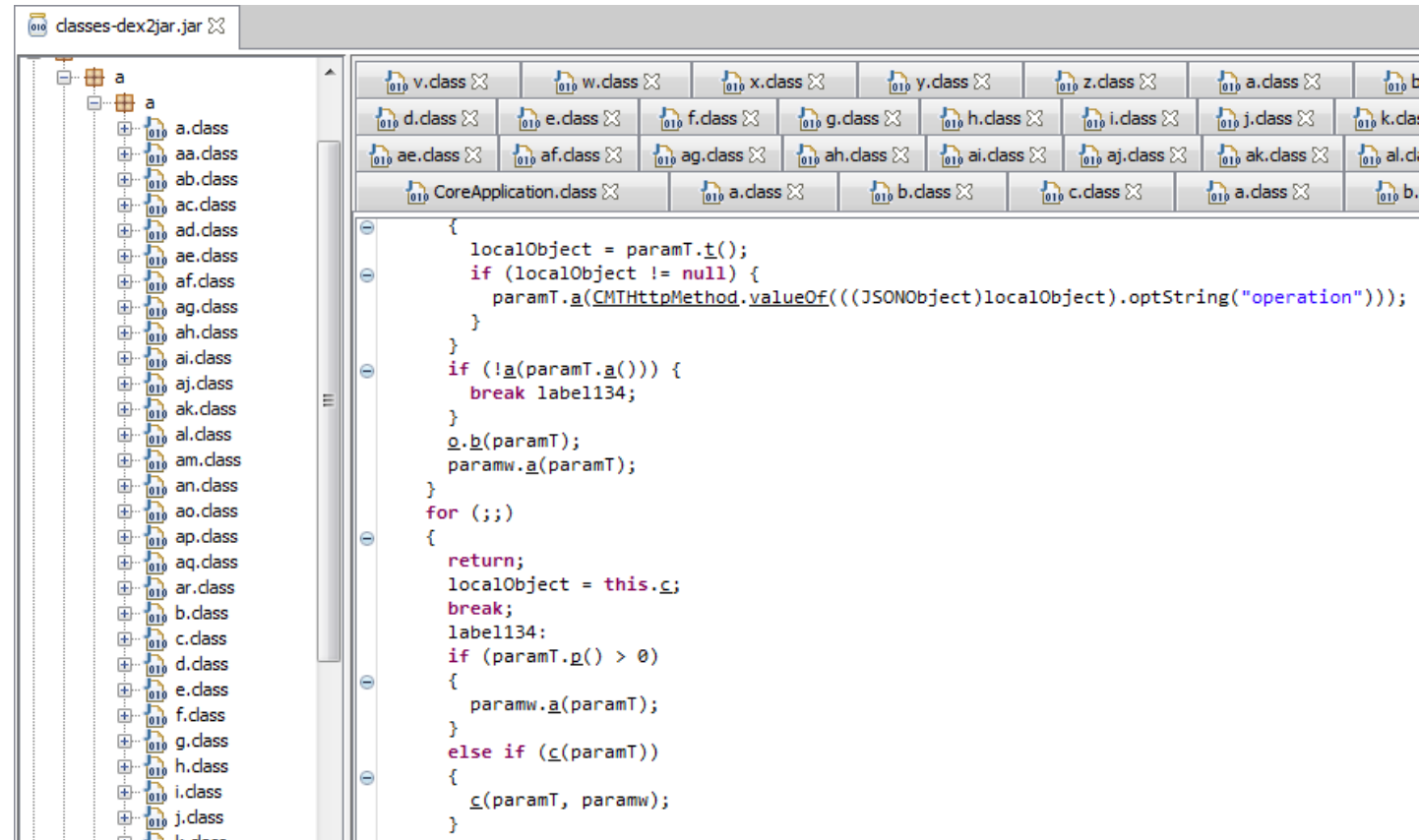
The screenshot shows the Yahoo! Finance mobile app interface. At the top, there is a search bar with the text 'Búsqueda de cotizaciones'. Below it, three market indices are displayed: BTC-USD (6,676.90, +4.91%), FTSE 100 (7,600.45, -0.80%), and Nikkei 225 (22,597.35, +1.85%). A section titled 'MIS POS. ACCIONARIAS/PART.' contains a progress indicator (10 black dots, the 10th is yellow with an exclamation mark) and two rows of data: 'Ganancia al día' (-0.38%) and 'Ganancia total' (-28.10%). Below this is a section 'MIS LISTAS'. At the bottom, there are two investment entries: 'MY INVESTMENTS' with a -0.38% change and 'Ally : Ally Account' with 0 symbols.

Asset	Value	Change
BTC-USD	6,676.90	+4.91%
FTSE 100	7,600.45	-0.80%
Nikkei 225	22,597.35	+1.85%

Metric	Value
Ganancia al día	-0.38%
Ganancia total	-28.10%

Investment	Change
MY INVESTMENTS	-0.38%
Ally : Ally Account	0 símbolos

- Obfuscation
 - To deter reverse engineering
 - Make it more difficult
- **Merrill Edge for Android:**



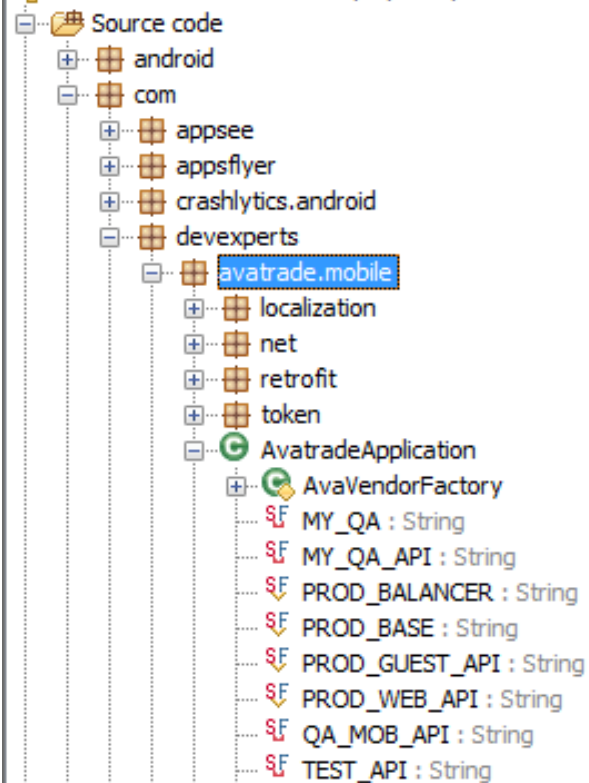
The screenshot shows a decompiler interface for a file named 'classes-dex2jar.jar'. On the left, a tree view lists classes from 'a' to 't'. The right pane displays the decompiled code for a class, showing obfuscated Java code with labels like 'label134' and 'label135'. The code includes a loop and several conditional statements with obfuscated method calls.

```
{
    localObject = paramT.ᵗ();
    if (localObject != null) {
        paramT.a(CMTHttpMethod.valueOf(((JSONObject)localObject).optString("operation")));
    }
}
if (!a(paramT.a())) {
    break label134;
}
ᵒ.ᵒ(paramT);
paramw.a(paramT);
}
for (;;)
{
    return;
    localObject = this.ᶘ;
    break;
label134:
    if (paramT.ᵑ() > 0)
    {
        paramw.a(paramT);
    }
    else if (ᶘ(paramT))
    {
        ᶘ(paramT, paramw);
    }
}
```

- 16 Android .apk installers (47%)
 - Reverse engineered **to human-readable code**
 - API keys
 - Private encryption keys
 - 3rd-party service partner passwords

```
nitr0us@bukowski:~/src/      $ grep -nir morningstar.com
com/                          .java:29:      MFProspectus.this.prospectusWebView.
loadUrl("http://      .morningstar.com/DocDetail.aspx?clientid= USER &key= PASSWORD &investm
enttype= &doctype=      &ticker=" + MFProspectus.this.getIntent().getStringExtra("symbol"))
;
nitr0us@bukowski:~/src/      $ █
```

- Dev/QA (internal) hostnames/IPs
 - 4 desktop platforms (29%)
 - 14 mobile apps (41%)



```
public class AvatradeApplication extends DXMarketApplication {
    private static final String MY_QA = "http://myqa2.avatrade.com:8022/";
    private static final String MY_QA_API = "http://myqa.avatrade.com:8023/api/";
    protected static final String PROD_BALANCER = "https://mobbalancer.avaapi.net/dxmobile-balancer/";
    protected static final String PROD_BASE = "https://mymob.avaapi.net/";
    protected static final String PROD_GUEST_API = "https://apimob.avaapi.net/v1/sso/";
    protected static final String PROD_WEB_API = "https://servicesmob.avaapi.net/api/";
    private static final String QA_MOB_API = "http://qamobapi.avatrade.com:8020/v1/sso/";
    private static final String TEST_API = "http://testapi.avatrade.com/v1/sso/";

    protected static class AvaVendorFactory extends VendorFactoryBase {
        private static final String PRIVATE = "-----BEGIN RSA PRIVATE KEY-----\nMIICWwIBAAKBggZiwmjV0w1BeuprcgVBSCz
        private static final String QA_PUBLIC = "-----BEGIN PUBLIC KEY-----\nMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgEr
        private final EnvironmentDescriptor mockDescriptor;

        protected int getLocalServerPort() {
            return 64100;
        }

        public AvaVendorFactory(Context context) {
```

```

nitr0us@bukowski:~/src$ egrep -hr "DEV_.*URL" RobinHood/
public static final String DEV_BROKEBACK_URL = "http://brokeback.dev.robinhood.com";
public static final String DEV_ANALYTICS_URL = "http://goku.dev.robinhood.com";
public static final String DEV_EXPERIMENTS_URL = "http://analytics.dev.robinhood.com";
nitr0us@bukowski:~/src$ egrep -hr "192.168. [0-9]{1,3}" Plus500/
private static final String d = "http://192.168. :40000/";
str = "http://192.168. :40000/";
str = "https://trade.plus500.com/".replace("trade.", "trade.test.").replace("trade.test.plus500.com", "192.168.: ');
nitr0us@bukowski:~/src$ egrep -hr "devexperts.com" Markets.com/
a(localLinkedHashMap, "CosmosStaging", "show.cosmos.prosp.devexperts.com:64000", "pre.cosmos.prosp.devexperts.com:64000");
a(localLinkedHashMap, "CosmosQA", "demo.qa.cosmos.prosp.devexperts.com:64000", "live.qa.cosmos.prosp.devexperts.com:64000");
a(localLinkedHashMap, "CosmosQARuslan", "demo.qa.cosmos.prosp.devexperts.com:64000", "89.113.133.21:64001");
a(localLinkedHashMap, "CosmosQAMike", "demo.qa.cosmos.prosp.devexperts.com:64000", "89.113.133.22:64001");
nitr0us@bukowski:~/src$ egrep -hr "scottrade.dev:8080" Scottrade/ | uniq
localURL2.<init>("http://gamobstrmpel01.scottrade.dev:8080");
localURL2.<init>("http://gamobdload001.scottrade.dev:8080/MobileServiceProxy/api/Pepperoni/POST");
localURL2.<init>("http://gamobdload001.scottrade.dev:8080/MobileServiceProxy/api/Pepperoni/DLY");
localURL2.<init>("http://gamobdload001.scottrade.dev:8080/MobileServiceProxy/api/Pepperoni/PRE");
localURL2.<init>("http://develictep002.scottrade.dev:8080");

```

```

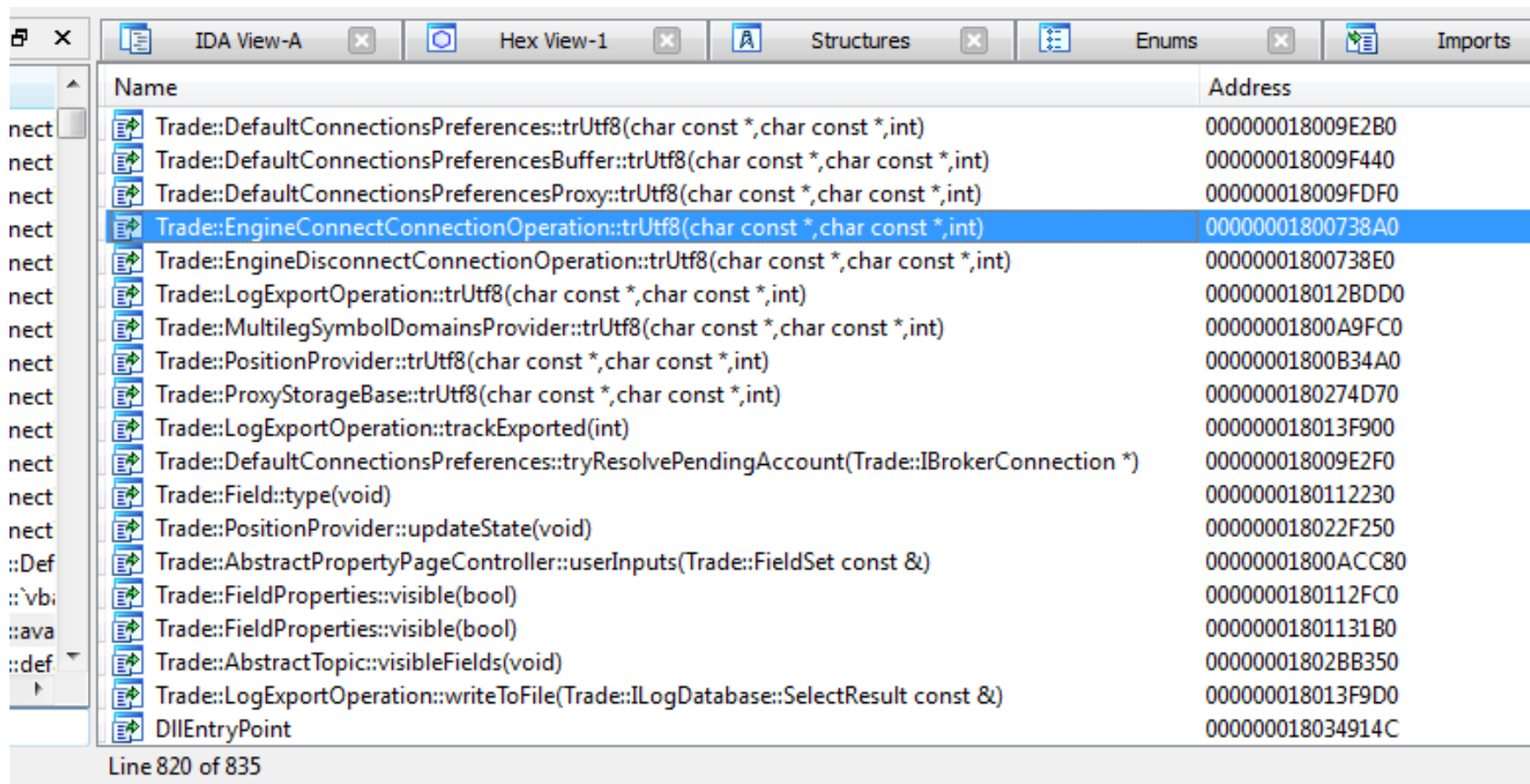
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .21"}}nitr0us@slacker:~$ curl https://us.etrade.com/apip
son -H 'consumerKey: 843c7d3799883583225a6a99a05a
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .23"}}nitr0us@slacker:~$
nitr0us@slacker:~$ curl https://us.etrade.com/apip
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .26"}}nitr0us@slacker:~$
nitr0us@slacker:~$ curl https://us.etrade.com/apip
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .22"}}nitr0us@slacker:~$ curl https://us.etrade.com/apip
son -H 'consumerKey: 843c7d3799883583225a6a99a05a
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .245"}}nitr0us@slacker:~$
nitr0us@slacker:~$ curl https://us.etrade.com/apip
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .23"}}nitr0us@slacker:~$
nitr0us@slacker:~$ curl https://us.etrade.com/apip
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .26"}}nitr0us@slacker:~$
nitr0us@slacker:~$ curl https://us.etrade.com/apip
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .21"}}nitr0us@slacker:~$ curl https://us.etrade.com/apip
son -H 'consumerKey: 843c7d3799883583225a6a99a05a
{"ClientRemoteAddressResponse":{"ipAddress":"10.5 .25"}}nitr0us@slacker:~$
nitr0us@slacker:~$

```



```
a.add(new co("Debug STE04 Platform", cp.c, "http://ste04lvtosapp01.iteclientsys.local:7001/Mobile", "STE04 Prod",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMV\\u0026o=220\\u0026p=https%3A%2F%2Finvest
));
a.add(new co("Debug STE04 Platform", cp.d, "http://ste04lvtosapp01.iteclientsys.local:7001/Mobile", "STE04 Demo",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMV\\u0026o=220\\u0026p=https%3A%2F%2Finvest
));
a.add(new co("Debug STE06 Platform", cp.c, "http://ste06lvtosapp01.iteclientsys.local:7001/Mobile", "STE06 Prod",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMV\\u0026o=220\\u0026p=https%3A%2F%2Finvest
));
a.add(new co("Debug STE06 Platform", cp.d, "http://ste06lvtosapp01.iteclientsys.local:7001/Mobile", "STE06 Demo",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMV\\u0026o=220\\u0026p=https%3A%2F%2Finvest
));
a.add(new co("Debug STE07 Platform", cp.c, "http://ste07lvtosapp01.iteclientsys.local:7001/Mobile", "STE07 Prod",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMV\\u0026o=220\\u0026p=https%3A%2F%2Finvest
));
a.add(new co("Debug STE07 Platform", cp.d, "http://ste07lvtosapp01.iteclientsys.local:7001/Mobile", "STE07 Demo",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMV\\u0026o=220\\u0026p=https%3A%2F%2Finvest
));
a.add(new co("Debug Local Platform", cp.c, "http://10.0.2.2:25006/Mobile", "Local Prod", "10.0.2.2:25005", "10.0.2.2:25005",
MV\\u0026o=220\\u0026p=https%3A%2F%2Finvest.tdameritrade.com%2Fgrid%2Fm%2Fola%3Fentity%3D103"));
a.add(new co("Debug Local Platform", cp.d, "http://10.0.2.2:25006/Mobile", "Local Demo", "10.0.2.2:25005", "10.0.2.2:25005",
MY\\u0026o=220\\u0026p=https%3A%2F%2Finvest.tdameritrade.com%2Fgrid%2Fm%2Fola%3Fentity%3D103"));
```

- Some executables/libraries with symbols



Name	Address
Trade::DefaultConnectionsPreferences::trUtf8(char const *,char const *,int)	000000018009E2B0
Trade::DefaultConnectionsPreferencesBuffer::trUtf8(char const *,char const *,int)	000000018009F440
Trade::DefaultConnectionsPreferencesProxy::trUtf8(char const *,char const *,int)	000000018009FDF0
Trade::EngineConnectConnectionOperation::trUtf8(char const *,char const *,int)	00000001800738A0
Trade::EngineDisconnectConnectionOperation::trUtf8(char const *,char const *,int)	00000001800738E0
Trade::LogExportOperation::trUtf8(char const *,char const *,int)	000000018012BDD0
Trade::MultilegSymbolDomainsProvider::trUtf8(char const *,char const *,int)	00000001800A9FC0
Trade::PositionProvider::trUtf8(char const *,char const *,int)	00000001800B34A0
Trade::ProxyStorageBase::trUtf8(char const *,char const *,int)	0000000180274D70
Trade::LogExportOperation::trackExported(int)	000000018013F900
Trade::DefaultConnectionsPreferences::tryResolvePendingAccount(Trade::IBrokerConnection *)	000000018009E2F0
Trade::Field::type(void)	0000000180112230
Trade::PositionProvider::updateState(void)	000000018022F250
Trade::AbstractPropertyPageController::userInputs(Trade::FieldSet const &)	00000001800ACC80
Trade::FieldProperties::visible(bool)	0000000180112FC0
Trade::FieldProperties::visible(bool)	00000001801131B0
Trade::AbstractTopic::visibleFields(void)	00000001802BB350
Trade::LogExportOperation::writeToFile(Trade::ILogDatabase::SelectResult const &)	000000018013F9D0
DllEntryPoint	000000018034914C

Line 820 of 835

- ASLR
- DEP
- Stack canaries

- **The majority of the desktop applications do not have these security features enabled in their final releases.**

- Similar mitigations on Linux

FileName	ARCH	ASLR	DEP	SafeSEH
C:\Program Files\Interactive Data\eSignal\whatsnew.exe	AMD64	True	False	N/A
C:\Program Files\Interactive Data\eSignal\esignal.exe	AMD64	True	False	N/A

FileName	ARCH	ASLR	DEP	SafeSEH
C:\Program Files (x86)\Common Files\Interactive Data\Options Analytix\Specs.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\DM\msvcp60.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\PT\2.0.4785.825\DEMOAPI.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\DM\winros.exe	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\DM\proxydll.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\DM\msvcrt.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\DM\mfc42.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\aesd.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\RIJNDAEL.DLL	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\PT\2.0.4785.825\PATSAPI.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\DM\implode.dll	I386	False	False	False
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiEft.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\ubsec.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\gmp.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\FRXC\2.0.4785.825\IndiForexCom.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\chil.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\capi.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\gost.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\padlock.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\MB\2.0.4785.825\IndiMB.dll	I386	False	False	True
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\IP\2.0.4785.825\IndiIP.dll	I386	False	False	True

```
nitroUs@ubuntu:~$ ./checksec.sh --dir /opt/iqoption/
```

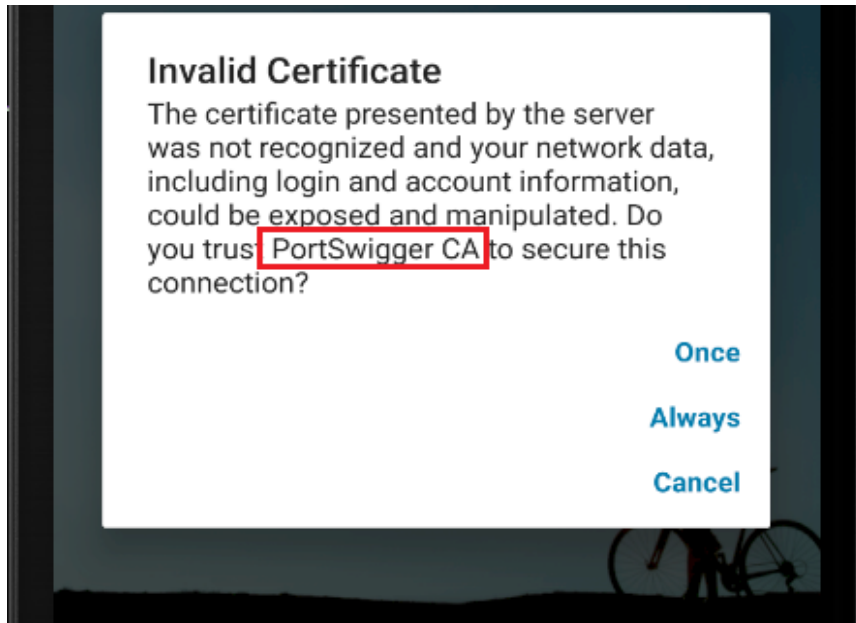
RELRO	STACK CANARY	NX	PIE	RPATH	RUNPATH	FILE
No RELRO	Canary found	NX enabled	No PIE	No RPATH	RUNPATH	/opt/iqoption/crashsender
No RELRO	Canary found	NX enabled	No PIE	No RPATH	RUNPATH	/opt/iqoption/IQOption
Partial RELRO	No canary found	NX enabled	DSO	No RPATH	No RUNPATH	/opt/iqoption/libc++.so.1

```
nitroUs@ubuntu:~$
```

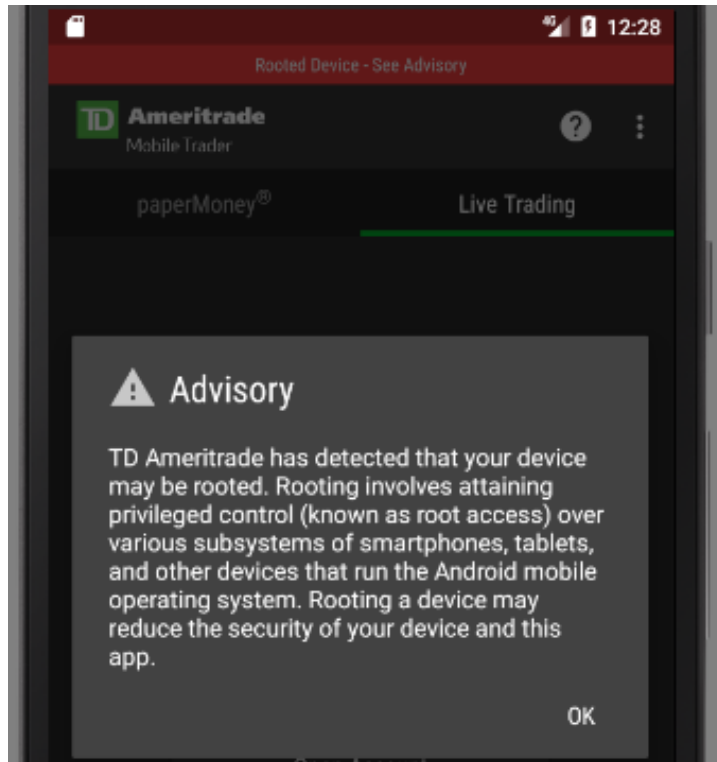
```
PS C:\Users\nitr0us\Downloads> Get-PESecurity -recursive -directory 'C:\Program Files (x86)\NinjaTrader 8' ; Where-Object {$_.ASLR -eq 'False' -or $_.DEP -eq 'False' -or $_.SafeSEH -eq 'False'} ; Sort-Object -Property ARCH ; Format-Table -Property FileName,ARCH,ASLR,DEP,SafeSEH
```

FileName	ARCH	ASLR	DEP	SafeSEH
C:\Program Files (x86)\NinjaTrader 8\bin64\msvcr90.dll	AMD64	True	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\pricehistorymgr.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\pricehistorymgr_shim.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\log4cplus.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\dbcapi_64UC8.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\ForexConnectShim.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\httpplib.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRT64Pro.dll	AMD64	True	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRT64Pro.dll	AMD64	True	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\Proxydll_64UC8.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\quotesmgr2_shim.dll	AMD64	False	False	N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\Specs.dll	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin64\dbcapi_UC8.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin64\proxydll.dll	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin64\Proxydll_UC8.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin64\NtDirect.dll	I386	False	True	True
C:\Program Files (x86)\NinjaTrader 8\bin64\IMPLODE.DLL	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin64\MetaLib.dll	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRTPro.dll	I386	True	False	False
C:\Program Files (x86)\NinjaTrader 8\bin\log4cplus.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\IMPLODE.DLL	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin\NtDirect.dll	I386	False	True	True
C:\Program Files (x86)\NinjaTrader 8\bin\MetaLib.dll	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin\dbcapi_UC8.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRTPro.dll	I386	True	False	False
C:\Program Files (x86)\NinjaTrader 8\bin\httpplib.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\ForexConnectShim.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\Specs.dll	I386	False	False	False
C:\Program Files (x86)\NinjaTrader 8\bin\quotesmgr2_shim.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRT.dll	I386	True	True	False
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRT.dll	I386	True	True	False
C:\Program Files (x86)\NinjaTrader 8\bin\pricehistorymgr_shim.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\pricehistorymgr.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\Proxydll_UC8.dll	I386	False	False	True
C:\Program Files (x86)\NinjaTrader 8\bin\proxydll.dll	I386	False	False	False

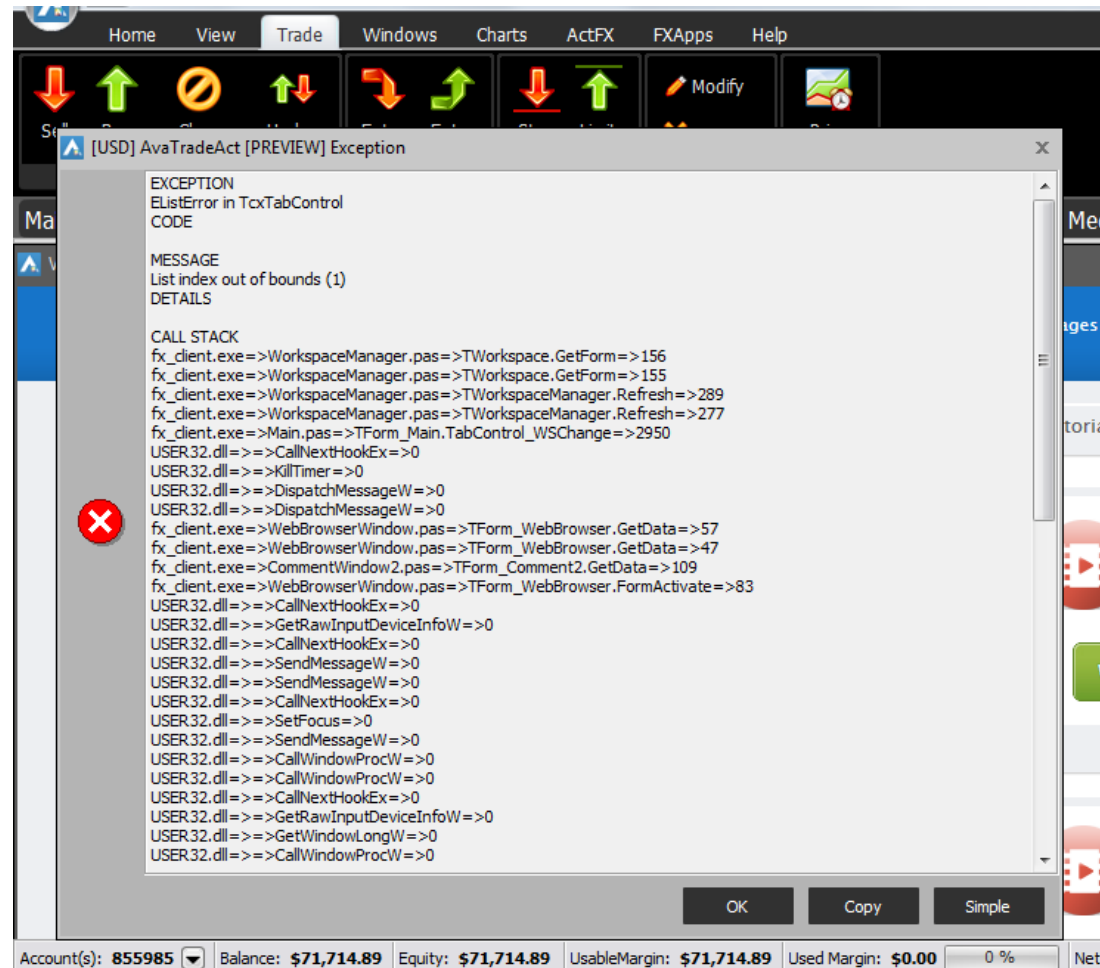
- 11 mobile apps (32%) do not validate it
 - *Man-in-the-Middle* (MiTM) attacks
 - From the ones that validate the SSL cert, only **Charles Schwab** allows the user to use the app with the provided certificate



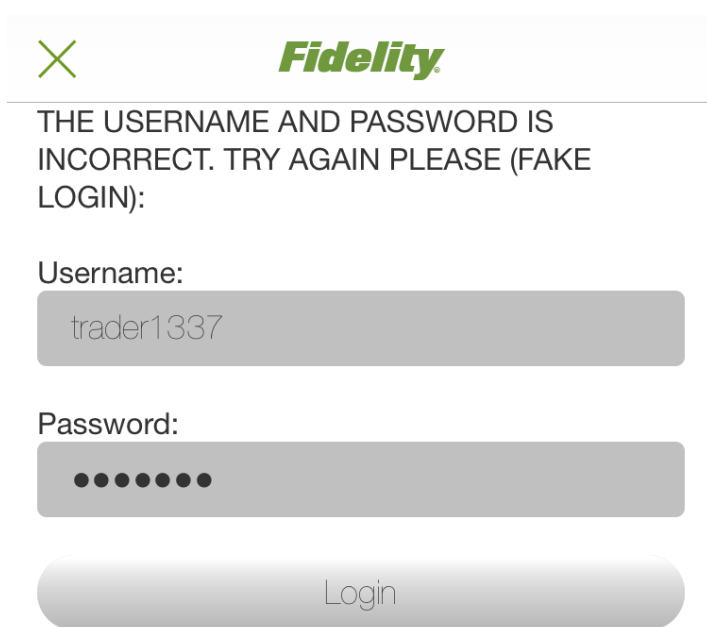
- 27 Android apps (79%) do not detect it
 - From the ones that detect it, only **TD Ameritrade** and **Thinkorswim** warn the user



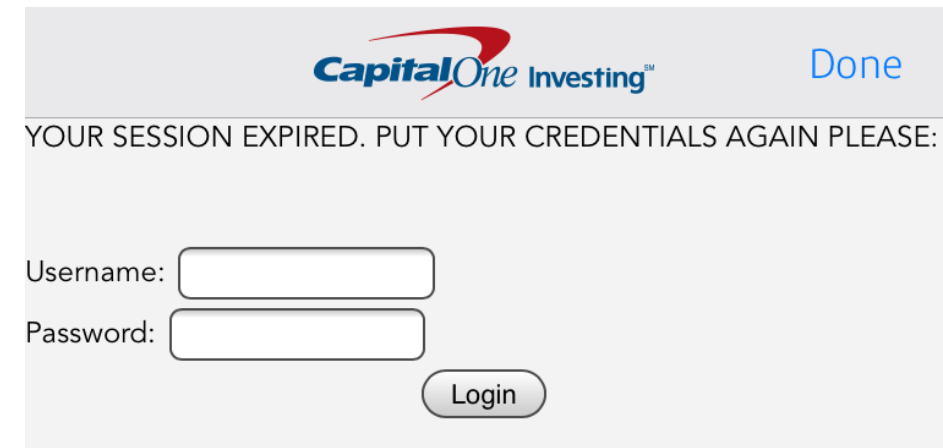
- Unhandled exceptions thrown to the user interface



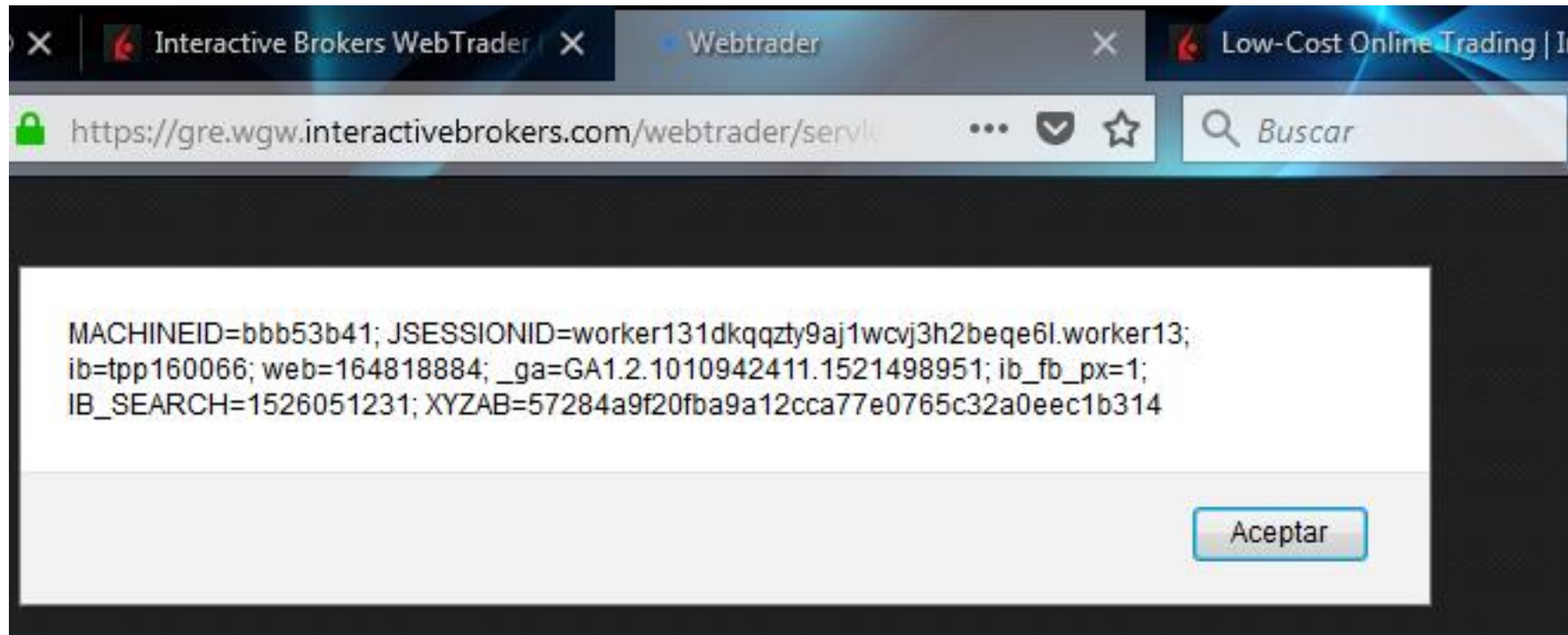
- Client-side data validation not performed
 - No sanitization against injected HTML/JavaScript code



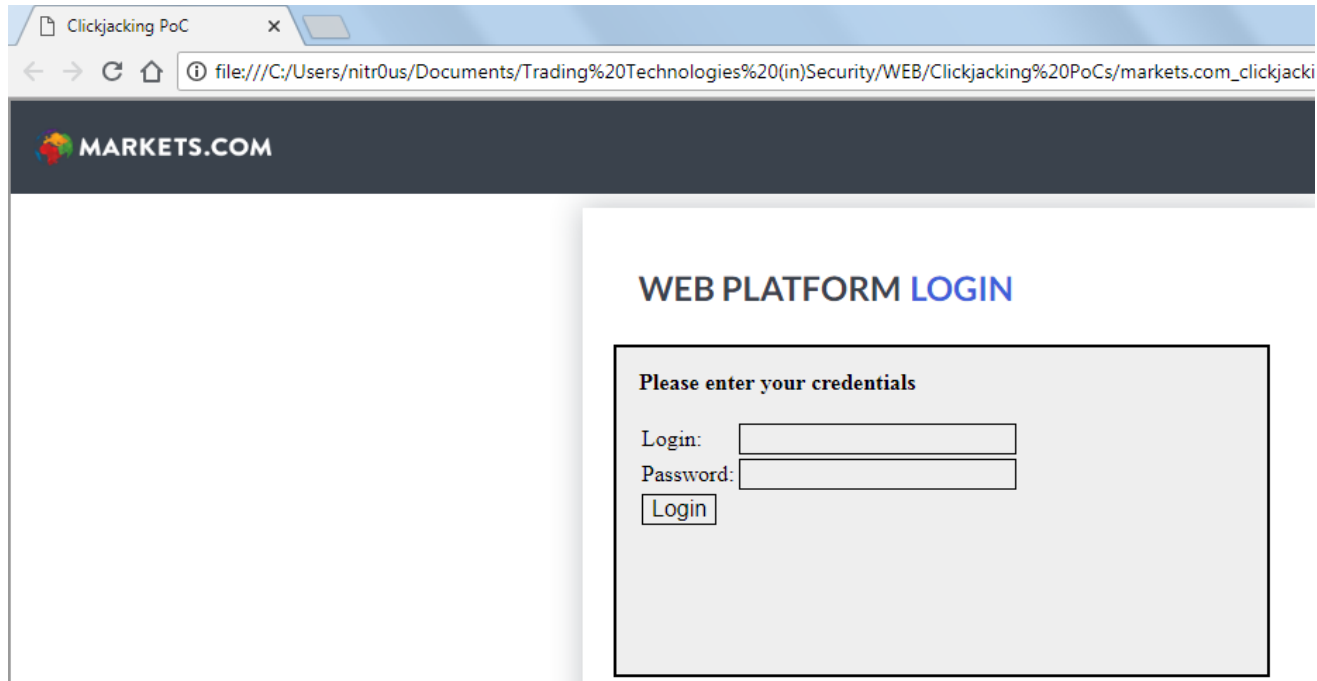
```
3A%5C%22OTHER%5C%22%2C%5C%22OffsitePlacemen%5C%22%3A%5C%22Unknown%5C%22%2C%5C%22PaidSearch%5C%22%3A%5C%22Unknown%5C%22%7D%22%7D%7D; PBELLA=|20170727.0|skins|bella-nav|bella2017-en_US.min.js|; et_segment=UCS- ST-CC- MOD- CIA-U IRA-N CSG- CT-; mmcore.tst=0.364; includesptab=n; _lang=es-MX; s_ppv=us.etrade.com%253Aaccounts%253Achangemyloginpassword%2C100%2C100%2C1461; LastSARCheckTime=1501525582898; LastUpdateTime=1501525582892; NextSARCheckMillis=30000; SessionExpirationTime=1501527352891; mmcore.et_funding=%7B%22brokerage%22%3A%7B%22value%22%3A%22CIA
```



- Cross-site scripting
 - **Interactive Brokers**



- Sensitive data in URLs
- Clickjacking
 - Personally, never heard of a real-life case



- Session cookies without `HttpOnly` / `Secure` in ~50% of the web platforms
- Lack of HTTP security headers in ~70% of the web platforms
 - `Strict-Transport-Security`
 - `Content-Security-Policy`
 - `X-XSS-Protection`
- Internal IP addresses and emails disclosure
 - HTTP response headers
 - HTTP body
 - JavaScript files

- Most brokers offer education on trading only
- No guidance on
 - General security
 - Privacy issues
 - Antivirus / Firewalls
 - Phishing
 - Contact emails to report something related
 - For example
 - **Firsttrade**
 - **TD Ameritrade**



Welcome to the Online Security Center



[How Firstrate protects your data](#)

[How to protect your personal information](#)

[How to deal with security threats to your account](#)

How to Deal With Security Threats to Your Account

Although scam artists try very hard to make fraudulent emails resemble official communication, there are often clues that will allow you to detect the scam. Here are some common characteristics of "phishing" emails, and how to determine if the email is authentic or a spoof.

If you suspect any fraudulent activity, please contact us immediately:

Telephone: 1-800-869-8800

Email: service@firstrate.com

Start by spotting the fraudulent communication.

- The email is completely unsolicited, from an address that looks legitimate (such as support@firstrate.com or feedback@firstrate.com).
- The email includes the logo graphics to convince reader of its authenticity, but has obvious typos and poor grammar.
- Content of the email lures the user to reply in order to confirm or verify personal information. This is usually done by conveying a sense of urgency, such as pointing out an error with the account that needs to be



Better protect yourself by understanding the threat

Knowing about possible online risks will help you better understand and recognize potential online threats to the security of your personal information. Your awareness, combined with our vigilance, can help to decrease the risk to your accounts and information.

[Avoid becoming a victim—use security products and tools](#)

[What to do if you suspect you're a victim](#)

Identity Theft

Identity theft—using a person's personal or financial data to commit fraud—is one of the most rapidly growing global crimes. The targets of this crime are your personal information, your financial information, and access to your online accounts.

The personal information often targeted includes:

- Name, address, and date of birth
- Social Security number
- Driver's license number
- Passport
- Signature

The financial information often sought is:

- UserIDs and passwords
- Account numbers and ABA numbers
- Credit card numbers

Asset Protection
Guarantee

Security Products

Our Security
Procedures

About Security Tools

Site & Browser
Settings

Minimum Requirements

Online Safety Tips

Online Threats

- > Security Issue
- > Spotting Phishing

- Please refer to the white paper for **more detailed vulnerabilities, screenshots and statistics**



- **Reported vulns to 13 brokers**
 - September 2017
 - May-July 2018

Broker	Date Reported	Status
TD Ameritrade	06-09-17	Reported
	25-05-18	Reported
Interactive Brokers	06-09-17	Reported
	18-05-18	Reported
Charles Schwab	06-09-17	Reported
	24-05-18	Reported
Plus500	06-09-17	Reported
	14-06-18	Reported
AvaTrade	06-09-17	Reported
	12-06-18	Contact initiated, no answer yet
IQ Option	06-09-17	Reported
	05-06-18	Contact initiated, no answer yet
Markets.com	06-09-17	Reported
	21-06-18	Contact initiated, no answer yet

- **Reported vulns to 13 brokers**
 - September 2017
 - May-July 2018

Broker	Date Reported	Status
Robinhood	06-09-17	Reported
eToro	06-09-17	Reported
E-TRADE	06-09-17	Reported
Capital One	06-09-17	Reported
easyMarkets	06-09-17	Reported
Firstrade	06-09-17	Reported
Grupo BMV	18-06-18	Contact initiated, no answer yet
Coinbase	17-07-18	Contact initiated, no answer yet
Yahoo! Finance	18-07-18	Reported
ETX Capital	19-07-18	Contact initiated, no answer yet
ETNA Trader	19-07-18	Contact initiated, no answer yet
OANDA	20-07-18	Reported
Money.Net	28-07-18	Contact initiated, no answer yet

- The brokers that communicated more with **IOActive**

- **TD Ameritrade**

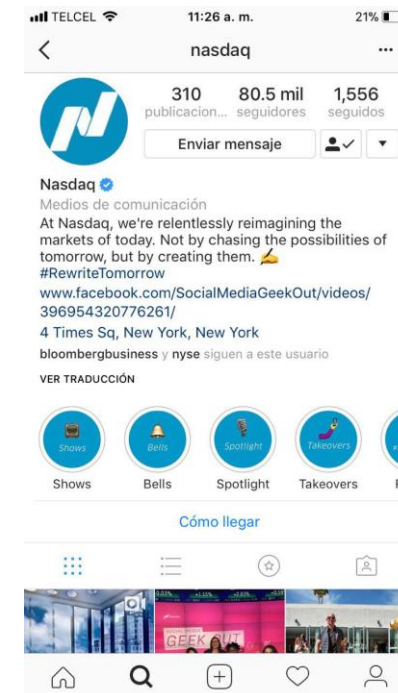


Ameritrade

- **Charles Schwab**



- **Social trading risks**
 - Some brokers implement social capabilities on their platforms
 - Copycat trading
 - Even the stock markets interact with people through social media



- **Social trading risks**
 - In addition to fundamentals and technical analysis tools
 - Sentiment analysis
 - Analyzes acceptance or rejection of certain securities by people



Nintendo Co Ltd OTC Pink - Current Information: NTDOY

Information Technology : [Software](#) | Large Cap Growth | Based in Japan [+ Company profile](#)

NTDOY

[Symbol lookup](#)

Postmarket	Last Trade	Change Since Close	Bid	Ask	B/A Size
	\$41.74	↓ -0.0615 (-0.15%)	0.00	0.00	0x0
July 17, 2018 4:02pm ET					

<input type="button" value="Buy"/>	<input type="button" value="Sell"/>	Closing Price	Day's Change	Bid	Ask	B/A Size	Day's High	Day's Low	Volume (Above Average)
		\$41.80	↓ -0.235 (-0.56%)	41.68	41.84	100x200	41.80	41.52	333,706
July 17, 2018 3:59pm ET									

[Set triggers](#) [Set alerts](#) [Add to watch list](#) [Historical quotes & splits](#) [Income Estimator](#) **NEW**

- Summary
- News
- Social Signals
- Charts
- Earnings
- Fundamentals
- Valuation
- Calendar
- Analyst Reports
- Peer Comparison
- SEC Filings

[Follow @TDameritrade](#) [Share your Twitter username](#)


Selected recent tweets ?

 **Steven Wang**
@stefanow777

Are adults who play 'Pokemon Go' hopeless slackers? |
[@guidelive p.d-news.co/nqsx](#)

1:38 PM - Jul 17, 2018

1  See Steven Wang's other Tweets 

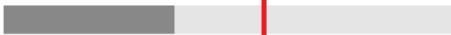
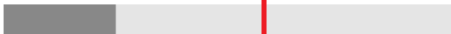
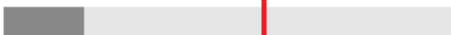
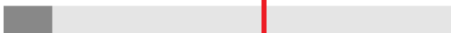
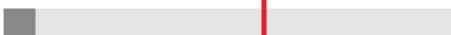
 **Random Wikipedia Ro**
@RandWikipediaRo

Game Boy Advance SP [wd52t.app.goo.gl/ALm84Joe1JLfcj...](#)

Social indicators

<u>7-day volume</u>	<u>Sentiment</u>
349,506	73.4%

Most-tweeted NTDOY brands ?

Pokemon	215.45K	
Nintendo	142.98K	
Pokemon GO	101.96K	
Mario	60.76K	
Zelda	40.87K	

Options: Enter underlying symbol and click Chain | Index: use "\$" (e.g. \$DJI)

- **Social trading risks**

- Trading on misleading information (i.e. fake news)
- Confusion

Twitter, Inc. (US) | https://twitter.com/search?q=%24PGP&src=typd

Momentos Notificaciones Mensajes SPGP

14 may.
Attention **SPGP** Users exploit has been found, check eff.org for more details.
Exploit paper released Trmw(5/15)
[\\$broken \\$hacked \\$attack eff.org/deeplinks/2018...](http://eff.org/deeplinks/2018...)

Traducir Tweet

1

14 may.
The Market is Open @themarketisopen - 14 may.
[\\$BPOP](#) [\\$BPOPM](#) [\\$BPOPN](#) [\\$MIME](#) **SPGP** Popular encrypted email standards are unsafe - European researchers

Traducir Tweet








The Market is Open
News ranking and comments for article Popular encrypted email standards are unsafe - European researchers







• Trading protocols

- Back office
- Stock exchanges
- Institutional trading

Americas [\[edit \]](#)

Exchange	Native Order Flow	FIX Order Flow	Market Data
Bolsa Mexicana de Valores	FIX	4.4 - version 2.4	INTRA / SIVA TCP
Boston Options Exchange	SAIL	4.2	HSVF
Chicago Mercantile Exchange	n/a	iLink	Simple Binary Encoding
Montreal Exchange	SAIL	4.2	HSVF
Nasdaq	OUCH 4.2  Client  [permanent dead link]	-	ITCH5.0 
NYSE	UTP Direct 	4.2  [permanent dead link]	
TSX	FIX  Client 	TSX-FIX	QUANTUMFEED
Aequitas Neo	FIX	FIX	NITCH

Europe [\[edit \]](#)

Exchange	Native Order Flow	FIX Order Flow	Market Data
Cboe Europe 	BOE	4.2	PITCH
Eurex	ETI	4.4	FIX/FAST
Euronext	UTP Direct	-	-
Borsa Italiana IDEM Derivatives	SAIL	4.2	HSVF
Liffe	-	-	-
London Stock Exchange	Millennium 	5.0sp2 	Level-2 ITCH Market Data
Moscow Exchange (MICEX)	MTESRL-TSMR	4.4	FIX/FAST
Moscow Exchange (RTS)	Plaza2	4.4	FIX/FAST
Oslo Børs (Derivatives)	SAIL 	4.2	HSVF
Oslo Børs (Equities)	Millennium	(5.0)	ITCH and FIX/FAST
London Stock Exchange UK Derivatives	SAIL (Native)	4.2	HSVF
Xetra	ETS	4.4	FIX/FAST

Asia [\[edit \]](#)

Exchange	Native Order Flow	FIX Order Flow	Market Data
Tokyo Stock Exchange	Arrowhead	4.2	FLEX

- No documents related to security
- General recommendations
- No guidance to FinTech companies



- **End users**

- Enable all the security mechanisms their platforms offer
 - 2FA
 - Biometric auth
 - Automatic logout/lockout
- Do not reuse passwords

- **Developers**

- Analyze your platforms
- Secure design/programming

- **Brokerage firms**

- Audit your applications internally and by 3rd-party companies



- Apparently, cybersecurity has not been on the radar of the **FinTech** space in charge of developing trading apps



- Correlation seen: **the biggest brokers are the ones that invest more in security**
 - Their products are more mature in terms of functionality, usability, and security

- Trading applications are less secure than retail banking.
- End users: enable all the security features provided by your broker.
- Brokers need to improve not only their trading applications, but also backend technologies for trading.

Thanks

Questions?

Alejandro Hernández ([@nitr0usmx](https://twitter.com/nitr0usmx))
Sr. Consultant

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

