



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

Alejandro Hernández ([@nitr0usmx](#))
Sr. Consultant



#BHUSA / @BLACKHAT EVENTS

IOActive
COMPREHENSIVE INFORMATION SECURITY SERVICES

About me

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



Agenda

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

Disclaimer

- 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**.









Introduction

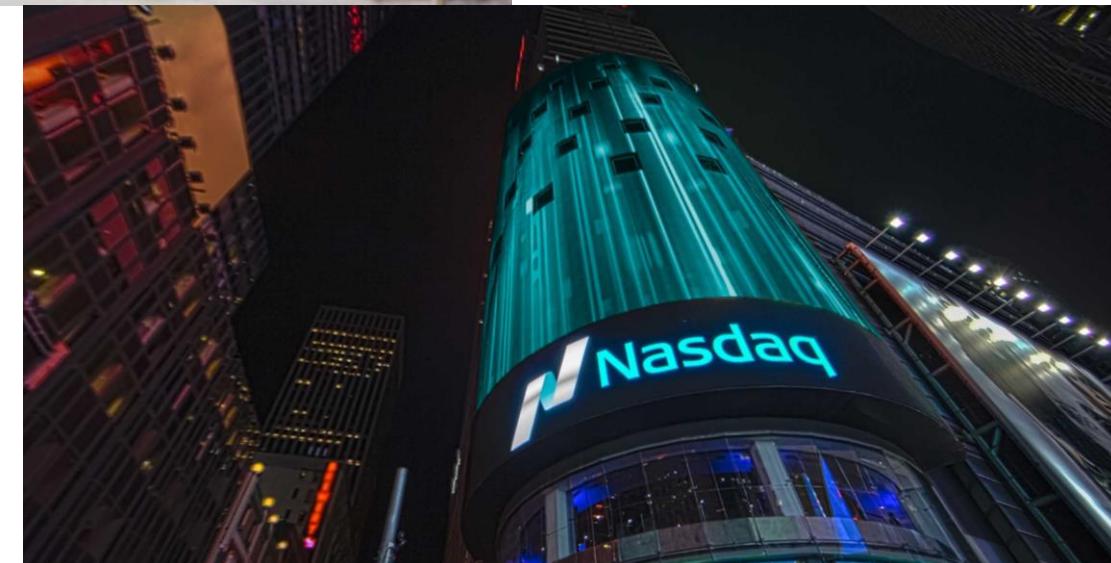
#BHUSA

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



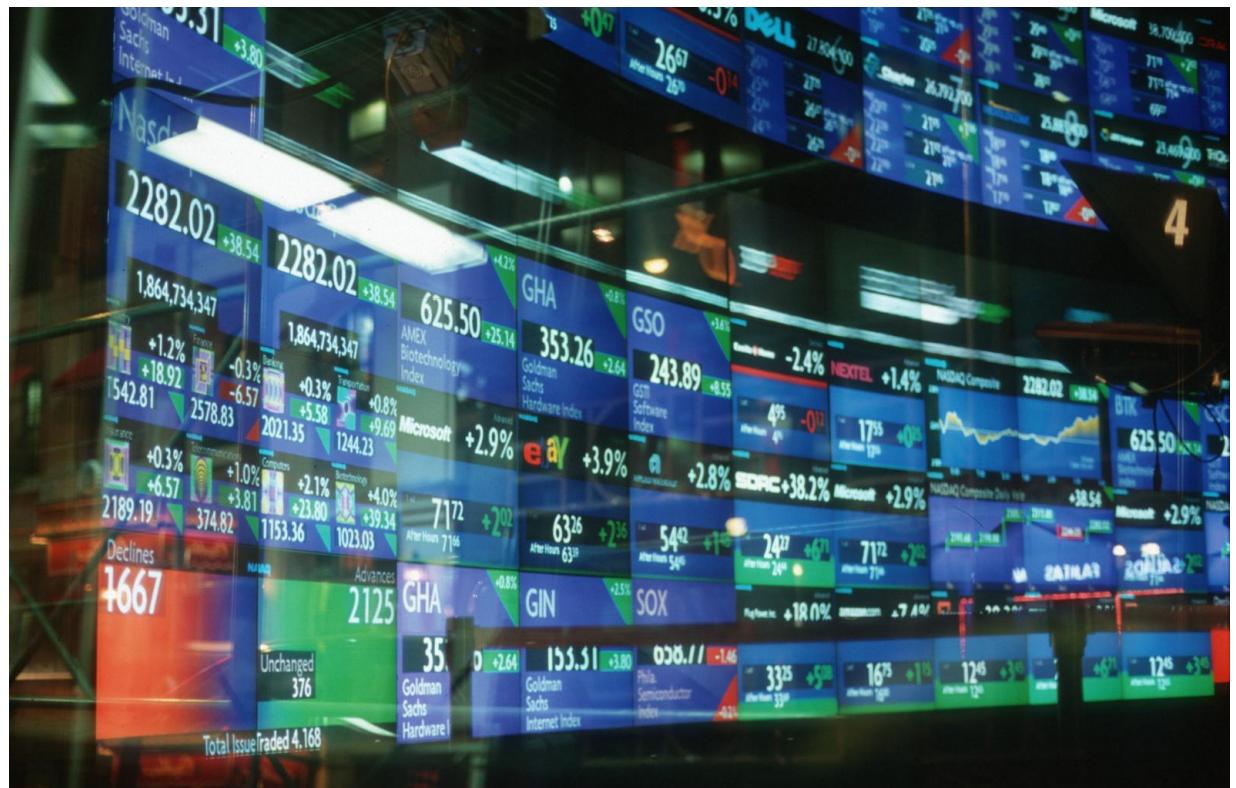
Introduction

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



Introduction

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



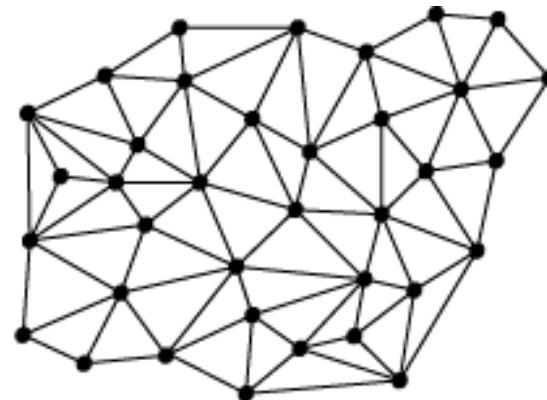
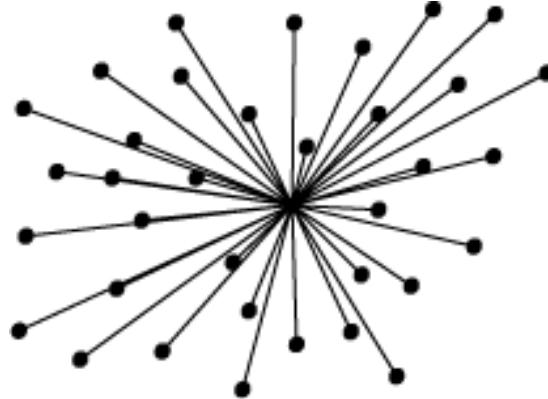
Introduction

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



Introduction

- 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.

Trading software

- 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



MetaTrader



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>

Trading software

#BHUSA

- 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



Bloomberg



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>

Trading software

#BHUSA

- 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/>

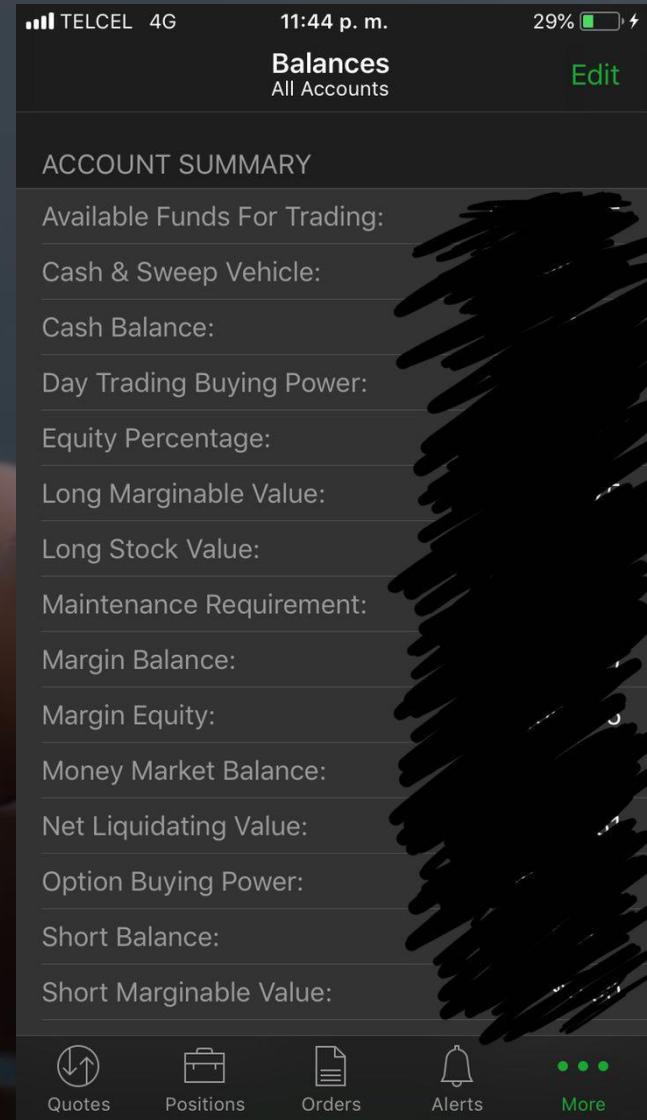
<https://ninjatrader.com/AboutUs>

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











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

Trading software

- 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
- Firstrade
- 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

Trading software

- 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]



Trading software

- 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

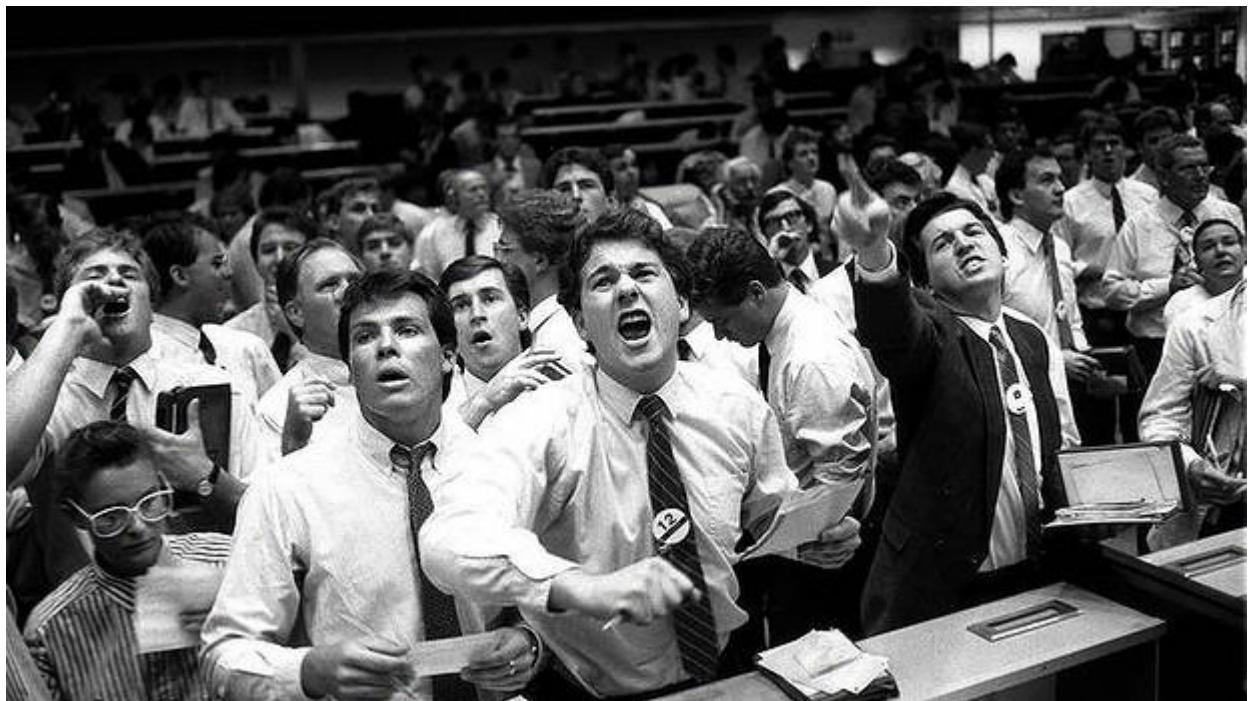
Mobile
Biometric authentication
Automatic logout/lockout for idle sessions
Privacy mode
Encrypted communication
SSL certificate validation
Session management
Client-side data validation
Sensitive data in logging console
Secure data storage
Root detection
App obfuscation
Hardcoded secrets in code

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](#).

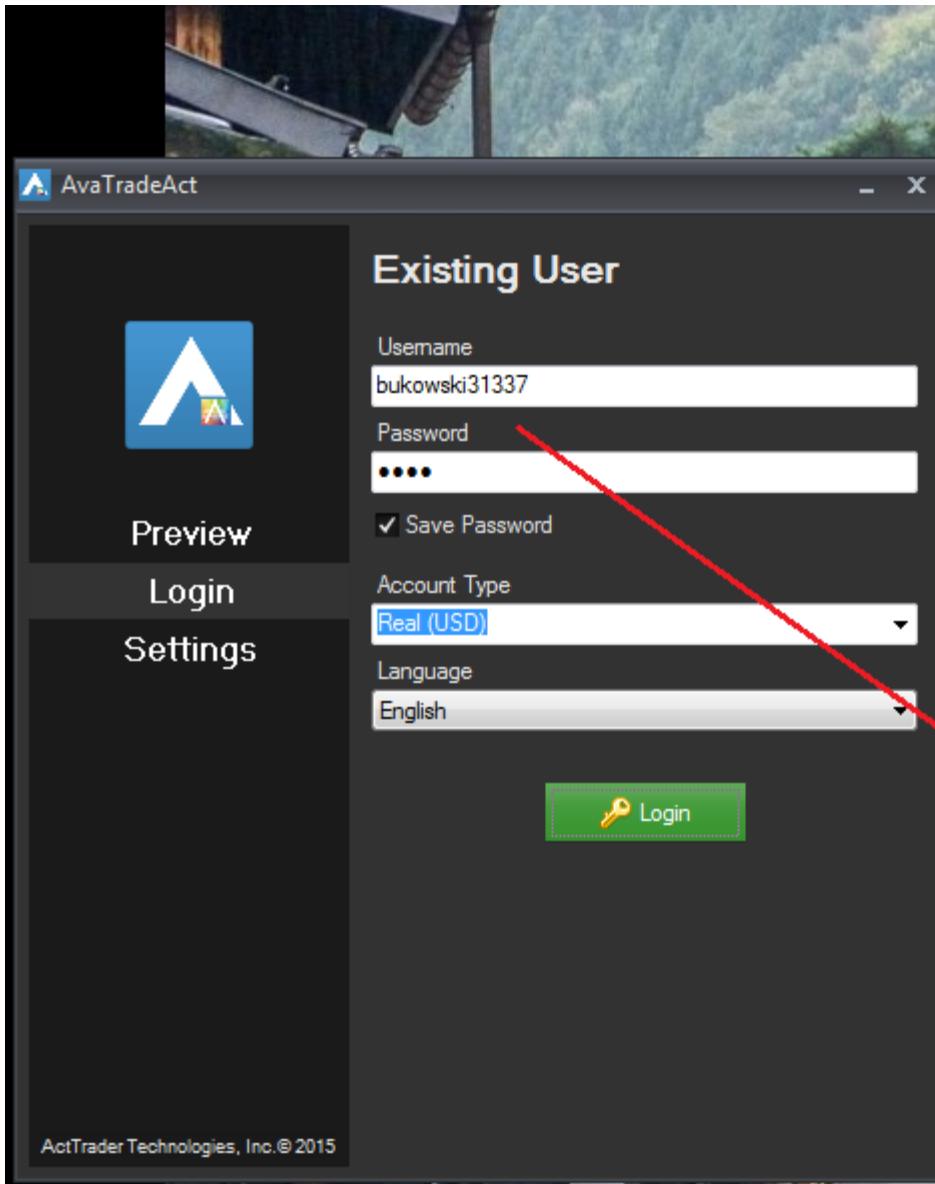
Results

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



Unencrypted comms

- **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: 3A2799F071009366FAACAA4FC91F2E8561A3739AC
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="gdUdrCw66bd6f480556af491f8cfce8c5719eae"
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: 3A2799F071009366FAACAA4FC91F2E8561A3739AC
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="gdUdrCw66bd6f480556af491f8cfce8c5719eae", algorithm="MD5", uri="/xml/logon?lang=en_US&secure=p&schema%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

Sell Buy New Chart Instrument Catalog Desktop Profile Indic Str

New Position

You will be Buying USD / Selling JPY

Instrument: USDJPY
Account(s): 855985
1,000 (radio button) 11,953,000
Amount: 3,000
Rate: 109.931
Trader Range: 0.0

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

```
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" ?>
```

[USD] AvaTradeAct [PREVIEW]

Home View Trade Windows Charts ActFX FXApps Help

Sell Buy New Chart Instrument Catalog

Trading Chart Instrument

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

Autochartist

Dealing Rates Table

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

autochartist.com™

Demo Account. Results are delayed.

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

actforex [Logout] English America/Sao_Paulo

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%2CUSDCNH%2CEURGBP%2CEURJPY HTTP/1.1
Timestamp: 2018-06-10 23:10:19.353
X-Auth-SHA1: 3312CA56369A723FBDA4899058BFE06A2EE5C045
Host: actforex.autochartist.com
Accept-Encoding: deflate, gzip, identity
User-Agent: FOREST 4.7.223.220/4.7.223

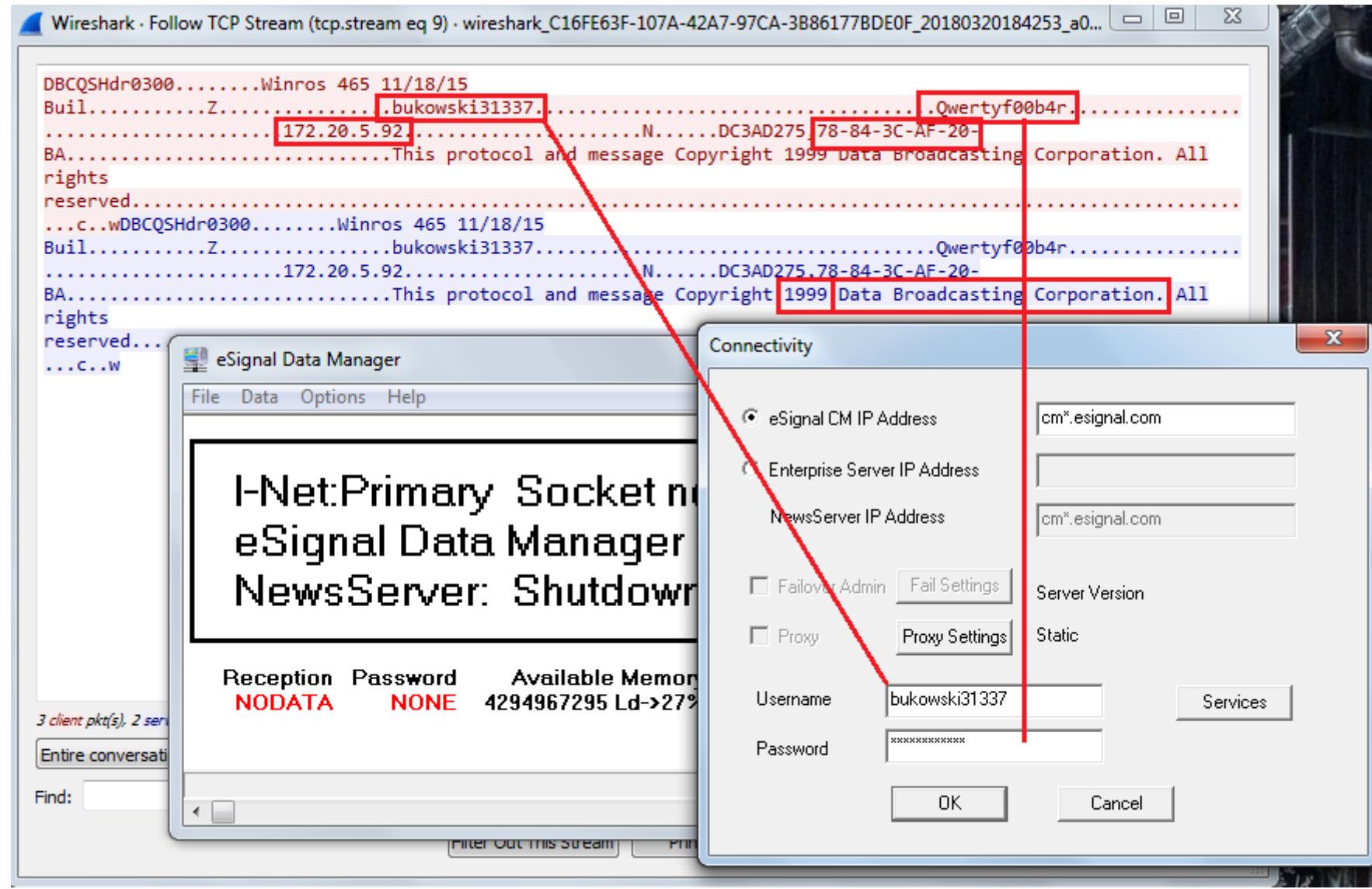
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=6FC971F118C85EDB738D1C561A78B63; Path=/aclite/; HttpOnly
Set-Cookie: rememberMe=deleteMe; Path=/aclite; Max-Age=0; Expires=Sun, 10-Jun-2018 03:09:50 GMT
Content-Type: text/xml
Transfer-Encoding: chunked
Date: Mon, 11 Jun 2018 03:09:49 GMT

<Authentication> <sessionid>6FC971F118C85EDB738D1C561A78B63</sessionid> <errormessage></
errormessage> <shorterrormessage></shorterrormessage> <mt4timezoneoffset>1000</mt4timezoneoffset>
<webapploginurl>http://actforex.autochartist.com/aclite/DirectMain?apiologintoken=qodfkOyoMaC9MSA50trqs004m4COVkB&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





3 de 53



Zoom automático

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 raised approximately \$43.2 million and invested approximately \$10.0 million in its operations. The Company engaged Merrill Lynch, Pierce, Fenner & Smith, Inc. to conduct an independent analysis of the Company's financial condition and to provide an opinion on the Company's financial statements.

Overview

The Company operates in two segments:

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

In the Institutional services segment, the Company provides action and descriptive information to major brokerage firms, insurance companies and pension funds. The Company also provides fixed income portfolio management services to pension funds and other institutional clients.



www.interactivedata.com/uploads/File/AnnualReports/idco_ar_01.pdf

14 de 54

IDC Annual Report 2001

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 inalámbrica

Wireshark · Follow TCP Stream (tcp.stream eq 25) · wireshark_C16FE63F-107A-42A7-97CA-3B86177BDE0F_20180320181944_a05...

File Edit View Go Cap

tcp.stream eq 25

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>

No. Time S...
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 on wire (365 bits), 457 bytes captured (365 bits)
Ethernet II, Src: Host (00:0c:29:14:00:00), Dst: cmfs.esignal.com (00:50:e8:03:36:67)
Internet Protocol Version 4, Src: Host (192.168.1.10), Dst: cmfs.esignal.com (192.168.1.11)
Transmission Control Protocol
[2 Reassembled TCP Segments]
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

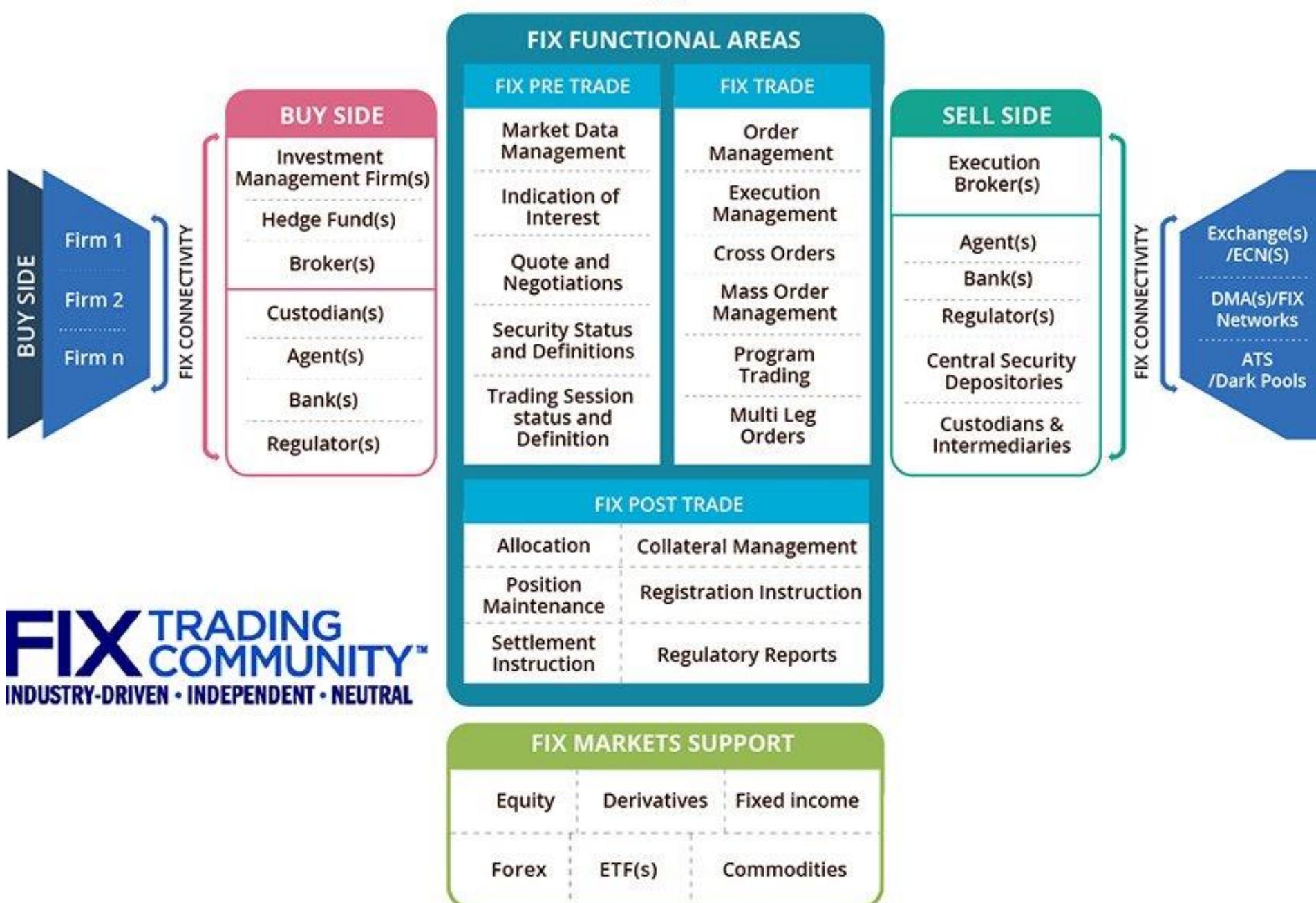
eSignal
eSignal cannot establish a connection due to internet connectivity issues or an invalid username/password.
User Name: bukowski31337
Password: *****
[Forgot your password?](#)
 Login Automatically
OK Cancel

- **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



FxPro
Trade Like a Pro

- 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)
SenderComplID: fxpro.10180548
TargetComplID: 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)
SenderComplID: fxpro.10180548
TargetComplID: 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



DEMO

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

100 LMT ▼ LMT PRICE 0.00 ▼ DAY advanced + SUBMIT



Login

User name bukow137

>Password

No user name? Try the demo

Trading Mode Live Trading

Color Palette dark

Use/store settings on server

Use SSL

More options Login Cancel

Monitor Portfolio Favorites US Movers + Filter ?

P&L + PROFILE Margin + ACCOUNT

DAILY -1,178 Unrealized 241.7K Net Liq 2.3M Excess Liq 1.7M Since prior Close -0.05% Maintenance 554.7K SMA 92.4K

POSITIONS My Positions by Strategy

	DLY P&L	POS	MKT VAL	LAST	AVG PX
My Investments	-6,245		994,156		
FSLR	-524	1,234	93,167	75.50	75.92 ^b
ISRG	-675	1,337	619,365	463.25	463.75 ^b
PLNT	-5,047	26,920	1,095,913	40.72	40.82 ^b
USD Cash			-814,289		

EE63F-107A-42A7-97CA-3B86177BDE0F_20180419102249_a03928

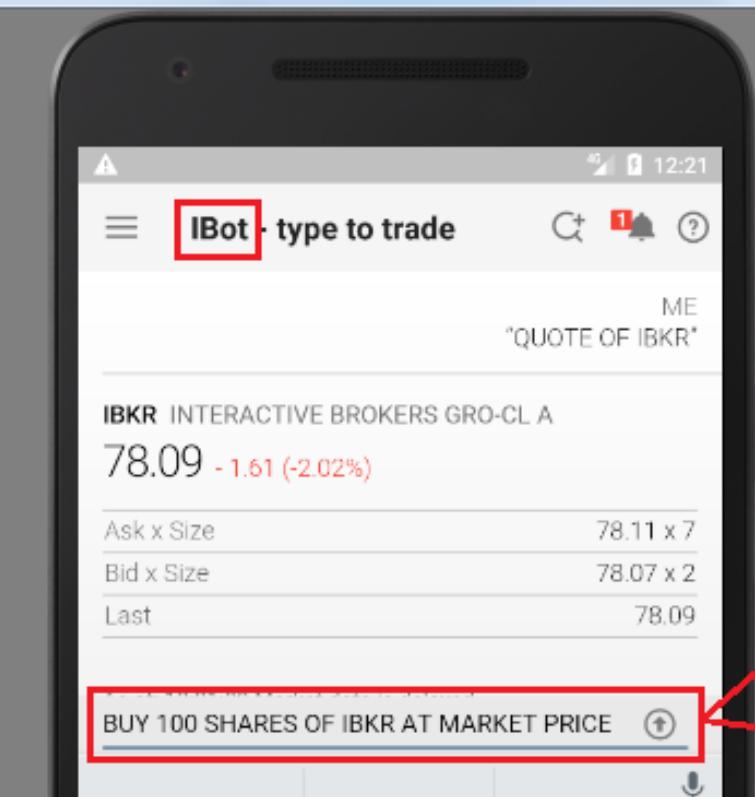
...@[.3@.....8=0.9=0024.35=G... .0D.@_.....8=0.
..a.@R.....8=0.9=0041.35=G... .\$.n.@Q.....0B.@H.E.....8=0.
.]n.0....(.,.\$.....q.Xn.....Q. .Bp....^@.b.^.....
.\\1..\$...1.Q....m...R.+o....
A*=D.!g...M...;D16x.^>.:1.... &.(.....+...p.,...c&q...)D`3....
y.....J.M...[.+.4kyv{.1...-o;V..&....n...]./.]....e....|.?:.K.....?'//.8=0.9=0027.35=Q.44714,193,0.01,0,0,9c,8=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 18Ku....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

102 client pkt(s), 810 server pkt(s), 161 turn(s).

10:31 a.m. jueves 19/04/2018

shares 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 Wal-Mart Stores", "Buy 100 shares of International 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,"buttonsPerPage":13>>@10=066@

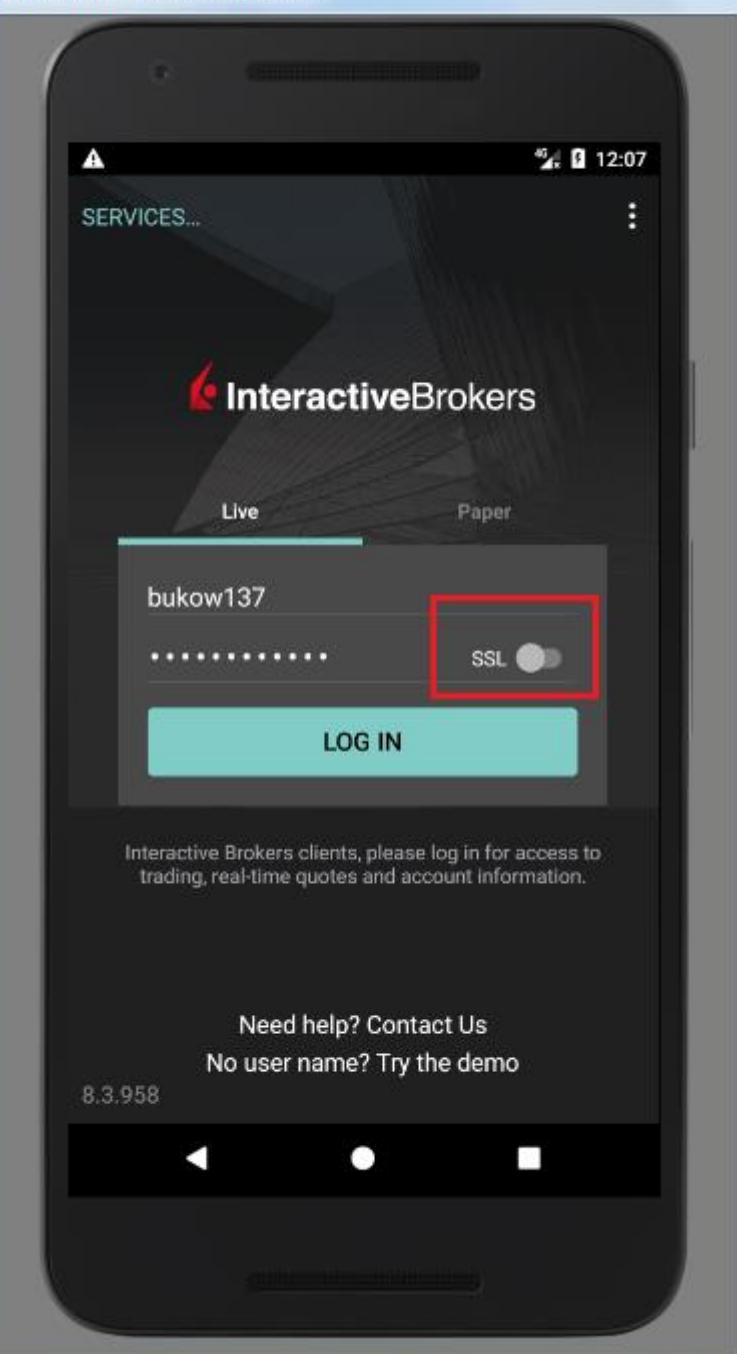
Android Emulator - nexus:5554



Bridge] : [OUT-0]: 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.....PJ....Rml>, "T": "Upcoming Earnings", "V": "2018050710293516", "D": "2018-05-07", "F": "Notify me of my holdings."}, "BN": 1, "T": "N", "U": 1}@0320=13@01: processJson: <"T": {"MO": 1, "E": [<"R": 0, "D": 1525696441, "MS": "IBKR FYI: Earnings Notification", "Content": "IBKR portfolio will announce earnings as below
 - PLNT declaring Q1 '18 earning on 2018-05-08"}, "Accounts": D****0182

Please see <a href="https://kb.clientam.com/vn/FN": "Upcoming Earnings", "I": "", "ID": "2018050710293516", "HT": 0, "FC": "EA", "FD": "Notify me of holdings."}, "D": 1, "T": "N", "U": 1}@01: not supported badge for launcher: com.google.android.apps.nexus.launcher@01: FYI: Received notification: FYINotification [id=2018050710293516, type=FYIPropertyType [07:34:51 CDT 2018, read=false, summary=[IBKR FYI: Earnings Notification], description=[Announce earnings as below
 - PLNT declaring Q1 '18 earning on 2018-05-08 AfterClose. Content: D****0182

Please see KB2133]}@01: 35=u@34=000003052=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","device":{"rasterWidth":256,"buttonsPerPage":5}}>@10=1251@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=120@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@01: [JavaBridge] : sendToNativeApp@01: 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@01: 35=mt@320=106@8082={"ok":1}@01: <"P":{}, "T": "IN", "U": 1}@01: 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=120@01: 35=mt@320=108@8082={"ok":1}@01: [JavaBridge] : sendToNativeApp@01: 8=FIX.4.1@9=0115@35=JP@320=109@6040=BOT@8082=<"T": "IN","P":<"text":"SUBMIT ORDER","device":{"rasterWidth":256,"buttonsPerPage":5}}>@10=228@



Account	
SIMULATED TRADING	
DU1010182	
All	
BALANCES	Margins Funds Mkt. Value
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

```

0x900 imply creation of host color buffer
Update:Allocation Details <
: ID=DU1010182+A+T,A>;accounts Codes:[DU1010182]
= []
D=DUC00074+A+S,A>=[Account[MGKS Asset Management - All, all
+M+S,A], Account[MGKS Asset Management - Core, alloc ID=DUC
182+A+S,A>= []
+T,A>=[Account[All, alloc ID=DU1010182+A+A,A], Account[My
C00074+A+S,A]
MODEL, ALL]>
Update:Allocation Details <
: ID=DU1010182+A+T,A>;accounts Codes:[DU1010182]
= []
D=DUC00074+A+S,A>=[Account[MGKS Asset Management - All, all
+M+S,A], Account[MGKS Asset Management - Core, alloc ID=DUC
182+A+S,A>= []
+T,A>=[Account[All, alloc ID=DU1010182+A+A,A], Account[My
C00074+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$2Ref654f3
@8082=<"a":"c","c":"63^7^8^4^4^84^65^66","t":"50822.6">@10
@5:d.b.a.b$1@2e42da?
: [main]: AccountListeners count@add>:6:d.b.a.b$1@2e42da?
I @T-2]: 8=FIX.4.1@9=0043@35=n@20=374@1=DU1010182+A+A@6040=B@7233=1@10=1,380
I @Tws : [IN-2-0]: 35=n@20=274@040-P@2119-Balance@@7121=Total USD@7100=Net Liquidation Value@7101=2,380
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
ties USD@7100=Net Liquidation Value@7101=2,380,002 @7100=Equity with Loan Value@7101=2,378,659 @7100=Previous
01=2,404,661 @7100=Securities Gross Position Value@7101=3,076,395 @7100=Cash@7101=-695,804 @7100=MTD Interest
Card Charges@7101=0 @7121=US Commodities USD@7100=Net Liquidation Value@7101=0 @7100=Equity with Loan Value@7
TD Interest@7101=0 @7100=Pending Debit Card Charges@7101=0 @
I Bloomberg: <"BBCL":"AQIAAAQeZRoUAF2X1ytBbPtHFE8sQAAAAAAAABAF5yQZ3FfSK9z+JCYQuMPaU6myJA2Uz1+p34wrUWHn+os4b0
xSzJE01A==">
```

The image shows two windows side-by-side. On the left is the 'Configuration' window of the Interactive Brokers application. It includes sections for 'Simplified user interface', 'Trade Buttons - Sell/Buy', 'Trouble Reporting' (with a red box around the 'Upload diagnostics' button), 'Debug mode', 'Extended log', 'Last farm' (showing email and IP), 'Server version' (Build 972.0i, May 10, 2018), and 'Interactive Brokers' (version 8.3.958). On the right is the 'Wireshark · Follow TCP Stream (tcp.stream eq 1)' window. It displays an ASCII dump of a POST request to 'cgi-bin/twserror.pl'. The request includes headers like User-Agent (Mozilla/5.0 Firefox/3.5.5), Accept, Accept-Encoding, Host, Accept-Language, Keep-Alive, Accept-Charset, Cache-Control, Connection, Content-Type, and Content-Length. Below the headers is a multipart form-data body with a boundary of '--1635fbf6d65'. It contains a file part named 'acct_id' with value 'bukow137', a file part named 'my_file' with value 'aTws_ULOG_20180514124250.tar.gz.zip', and a binary file part. A red box highlights the 'Content-Disposition' header for 'acct_id' and the 'Content-Disposition' and 'Content-Type' headers for 'my_file'.

```
POST /cgi-bin/twserror.pl HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 206.106.137.34
Accept-Language: en-us,en;q=0.7,ru;q=0.3
Keep-Alive: 300
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=-----1635fbf6d65
Content-Length: 81699

-----1635fbf6d65
Content-Disposition: form-data; name="acct_id"
bukow137
-----1635fbf6d65
Content-Disposition: form-data; name="my_file";
filename="aTws_ULOG_20180514124250.tar.gz.zip"
Content-Type: application/x-zip

.....v.F.(....Z...{./33.3.....|.H..X"....x.Z. J.y3AYV...Y.<.y.svU7.6@..
$..I..g".....TWWNUlw'..?.....P.4M.,K._M.S...Pm.0....
```

Watch List

My Positions TO INVEST LATER

#	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

SPOT Go 150.80 ▼ -7.96 (5.01%) Spotify Technology

Extended Hours: 151.49 ▲ +0.690 (0.46%)

SPOT : 1 Year : Daily

1 Year : Daily

Realized Gain/Loss

Refresh Action

There are no positions.

Quick Jumps Date Range

Link

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.
.#.0.:|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...$.....2.S.u...}(k..j+N?.....0....=
....T.6.U..T4...G*j.....{`.../K_WLXx.*....0...'5..%Xw
n.unW...>,...j.n....H1...H...m}~...smo...XF"+_;at.D".~;
T.n#..../o.E|x...Qq...
...1.....J|x.3. ....K....?..q#.;D|x...Qq...
...1.....:|x.....ak|x.3....q....12.1M.1...H...Og...
.&FF.)@.1` .....18.2|1|SPOT|
44_|1|SPOT|
G4`|1|SPOT|
{"Advise":3001,"Echo":305,"SymbolArray":["SPOT"]}
14b|1|SPOT|
R|1|SPOT
Q|307|SPOT|180518|0000|190518|1259|1|1
Q|308|SPOT|180518|0000|180518|1619|1000|1
5o|x.uQMo.0...WX9...";...4eK.|.$DB ..vE....4...=l...."...
80 client pkt(s), 474 server pkt(s), 87 turn(s).
Entire conversation (77 kB)
Find:
Filter Out This Stream Print Save as...
```

Current build: 1.54.89.0 100% Hide Balances

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

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

News Last Trade Change % Change

	150.55	-0.25	-0.17	1
	328.87	+4.69	+1.45	3
	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		

+0.3514 (0.71%) Okta Inc

50.75
50.50

Add Group Sync Off Actions

Stock/ETF Calls/Puts Conditional Orders Actions

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|
411|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>caten -nir 59db7ec25f4d3ad83fb8a71cef701ac *
cfg.dat:1:{ "ssid": "59db7ec25f4d3ad83fb8a71cef701ac", "user_id": 21519658, "locale": "en", "user_locale": "en_US", "itrousenador@gmail.com", "token": "8d94eab5b2137dd8004cd4606c05532081c8940791f3a7efdef031468375f379be68a4b78caa7a8182736e0bfc933d62a", "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"}
```

```
C:\Users\nitr0us\AppData\Roaming\IQ_Option>
```

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=59db7ec25f4d3ad83fb8a71cef701ac; 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.com", "last": "0", "log": "0", "logLevel": "0", "logType": "0", "mac": "0", "platform": "0", "port": "0", "proxies": "0", "script": "0", "version": "0"}, "time": "2018-04-02T17:48:20Z"}]
```

NINJATRADER

New

Tools

Workspaces

Connections

Help

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

nitr0us@bukowski:~\$

```
nitr0us@bukowski:~$ nc 192.168.241.1 36973 -v
Connection to 192.168.241.1 36973 port [tcp/*] succeeded!
20Orders|2Strategies|2BuyingPower|02CashValue|1000002RealizedPnL|02Orders|Sim1012Strategies|Sim1012BuyingPower|Sim10102CashValue|Sim101100000|RealizedPnL|Sim10102Orders|Account12Strategies|Account12BuyingPower|Account102CashValue|Account11000002RealizedPnL|Account102Orders|Account32Strategies|Account32BuyingPower|Account302CashValue|Account3100000|RealizedPnL|Account302OrderStatus|67fd54f568874b969c9087cedbcb0bf3Rejected2Filled|67fd54f568874b969c9087cedbcb0bf302OrderStatus|8d9b9e8aaa0c4c2e8b883f497e0988b1Rejected2Filled|8d9b9e8aaa0c4c2e8b883f497e0988b102AvgFillPrice|8d9b9e8aaa0c4c2e8b883f497e0988b102OrderStatus|074893f5ce804a39add9d1483da0d0baRejected2Filled|074893f5ce804a39add9d1483da0d0ba02Orders|Secret Account2Strategies|Secret Account2BuyingPower|Secret Account02CashValue|Secret Account233000|RealizedPnL|Secret Account02ATITrue
```

^C

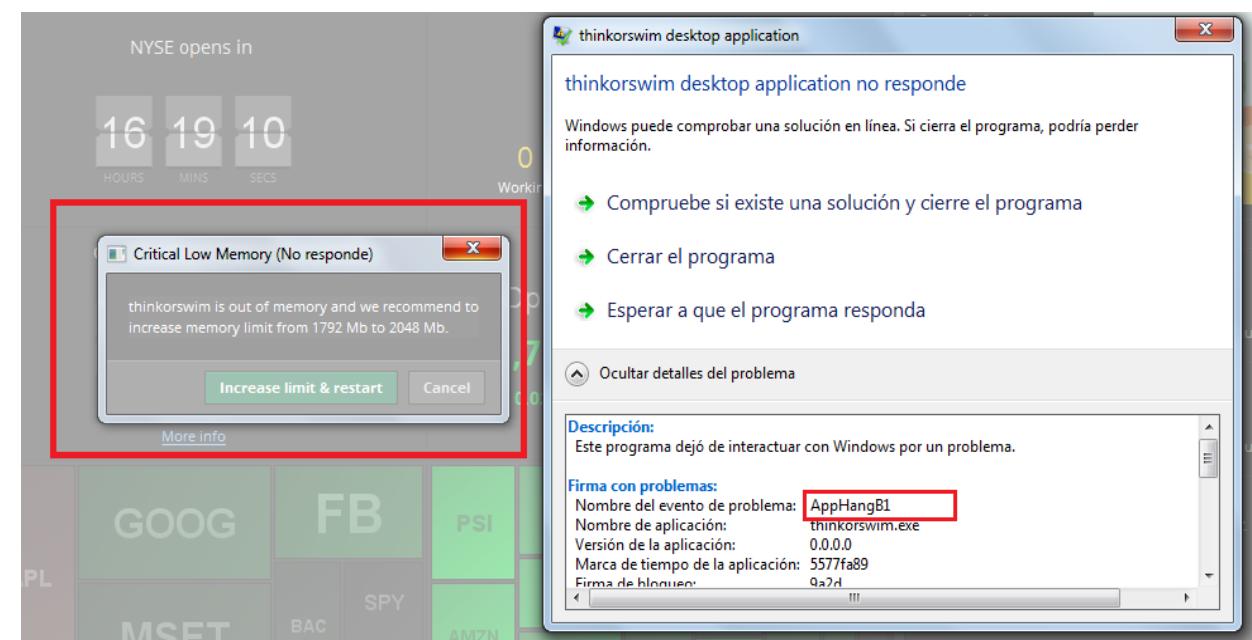
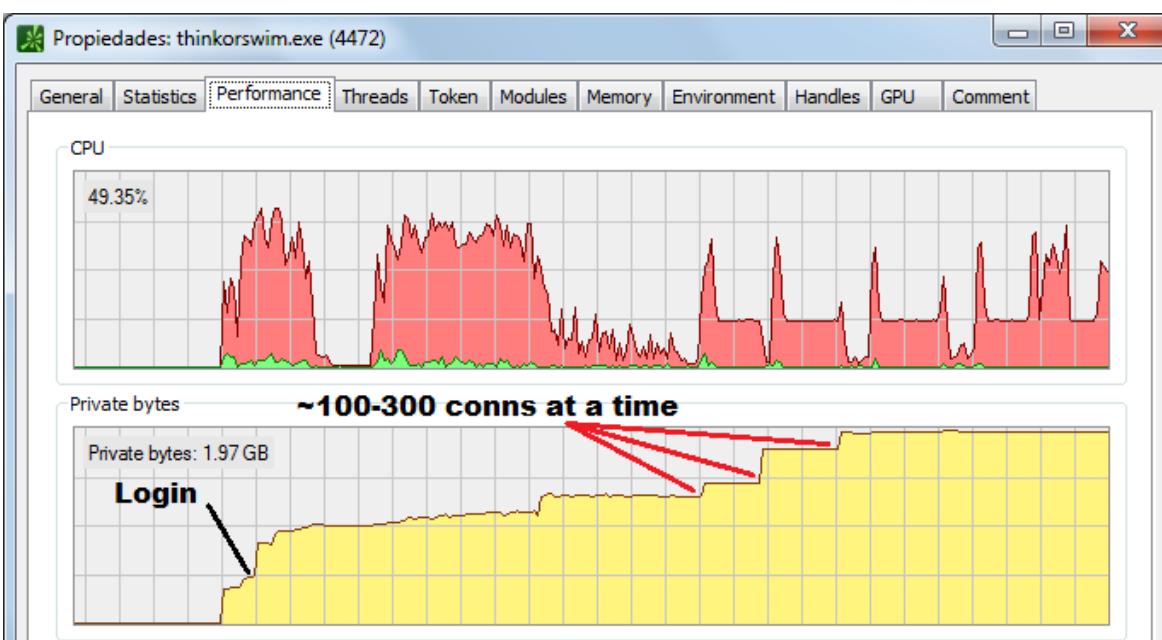
nitr0us@bukowski:~\$

Denial of Service

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

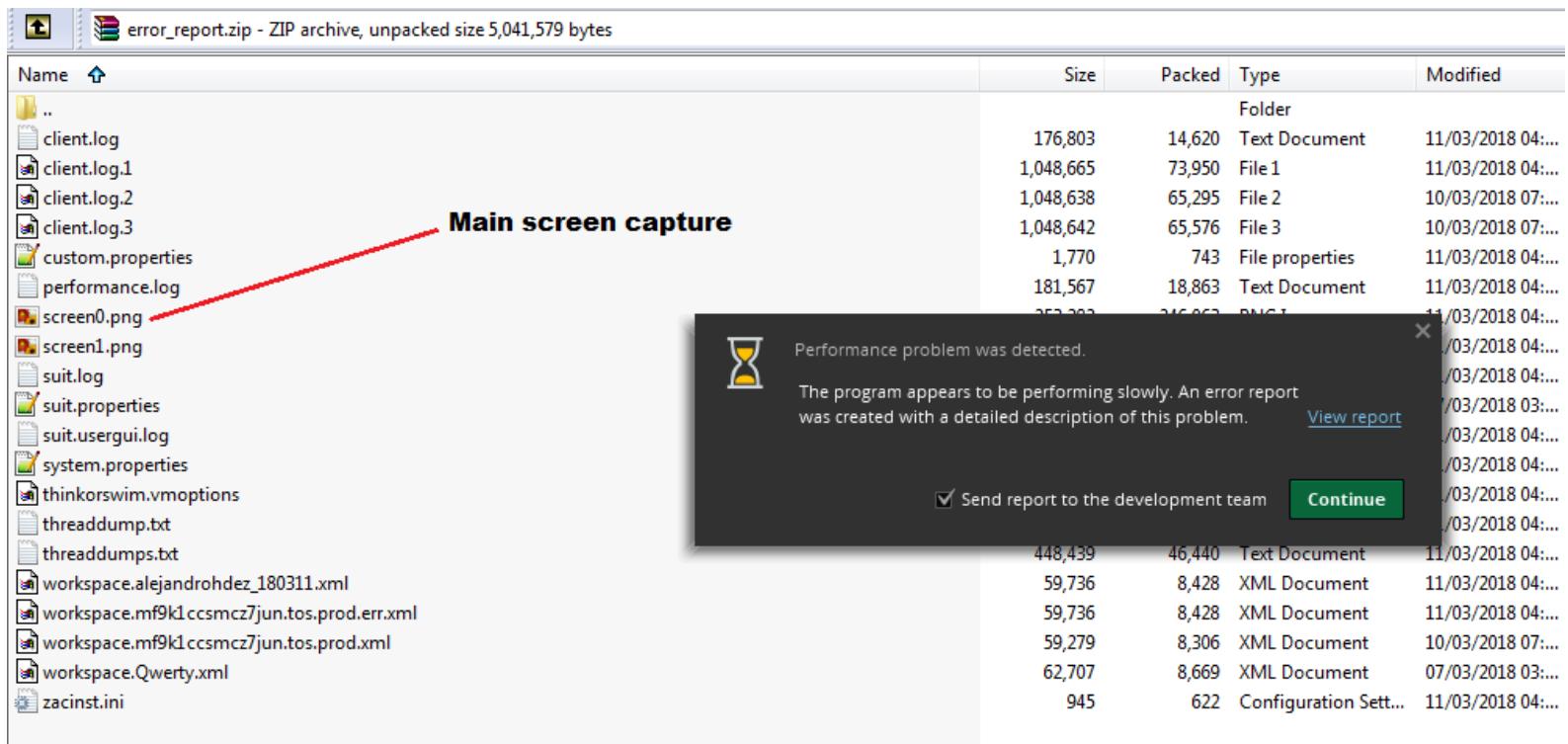
Denial of Service

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



Denial of Service

- 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?



SIMULATED TRADING Connected Friday, Mar 16, 2018 Account: PAPER (REAL ACCOUNTS) Home Screen Messages Support Chat Setup

Account Info

- Option Buying Power \$165,844.04
- Forex Buying Power \$10,000.00
- Net Liq & Day Trades \$196,237.26
- Cash & Sweep Vehicle \$135,450.83

thinkorswim

Paper@thinkorswim [build 1924]

Live News

Time Title (Click to sort)

- 13:46:15 BZ: PCTE
- 13:45:44 ADBE, Q
- 13:45:33 Eastman
- 13:45:24 BZ: OvaS
- 13:45:00 MW UPD
- 13:45:00 IGT Post
- 13:45:00 Winston
- 13:45:00 Dow Jon

Watchlist Top1

Symbol	Last	Change	Volume	Open
DXR	13.35	+5.5501	21.66	8.05
OSN	3.10	+.45	3.30	2.58
JNP	12.50	+1.10	12.65	11.00
INO	4.84	+.37	4.90	4.29
PTI	7.08	+.525	8.61	6.82
MHH	14.77	+1.08	15.00	13.76
NES	22.00	+1.58	22.00	20.46

Quick Chart on ISRG

ISRG 441.95 +1.18 +0.27% D

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

5
0 Working 3 Filled 2 Canceled

IFLX 321.00

CBOE (Chicago) 3:47 PM OPEN
FWB (Frankfurt) 9:47 PM
NYSE (New York, USA) 4:47 PM

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

Econoday event

Current account... AMX 19.23 -.10 (-.52%) CIBR 25.91+.05 (+.19%) EWW 50.86

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());
            if ((ch = s.charAt(++idx)) == ')')
                break;
            ch = s.charAt(++idx);
            while (ch == ' ')
                ch = s.charAt(++idx);
        }
        if (closure + 1 == s.length())
            return "";
        if (ch == ',')
            if (closure + 1 == s.length())
                return "";
        if (closure + 1 == s.length())
            return "";
    }
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' '))
        if (s.charAt(closure + 1) != ' ')
            return null;
    return s.substring(closure + 1);
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' '))
        if (s.charAt(closure + 1) != ' ')
            return null;
    return s.substring(closure + 1);
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' '))
        if (s.charAt(closure + 1) != ' ')
            return null;
    return s.substring(closure + 1);
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' '))
        if (s.charAt(closure + 1) != ' ')
            return null;
    return s.substring(closure + 1);
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' '))
        if (s.charAt(closure + 1) != ' ')
            return null;
    return s.substring(closure + 1);
}

private String parseSuffix(String s) {
    int idx = 0;
    int len = s.length();
    while ((idx < len) && (s.charAt(idx++) == ' '))
        if (s.charAt(closure + 1) != ' ')
            return null;
    return s.substring(closure + 1);
}
```

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.

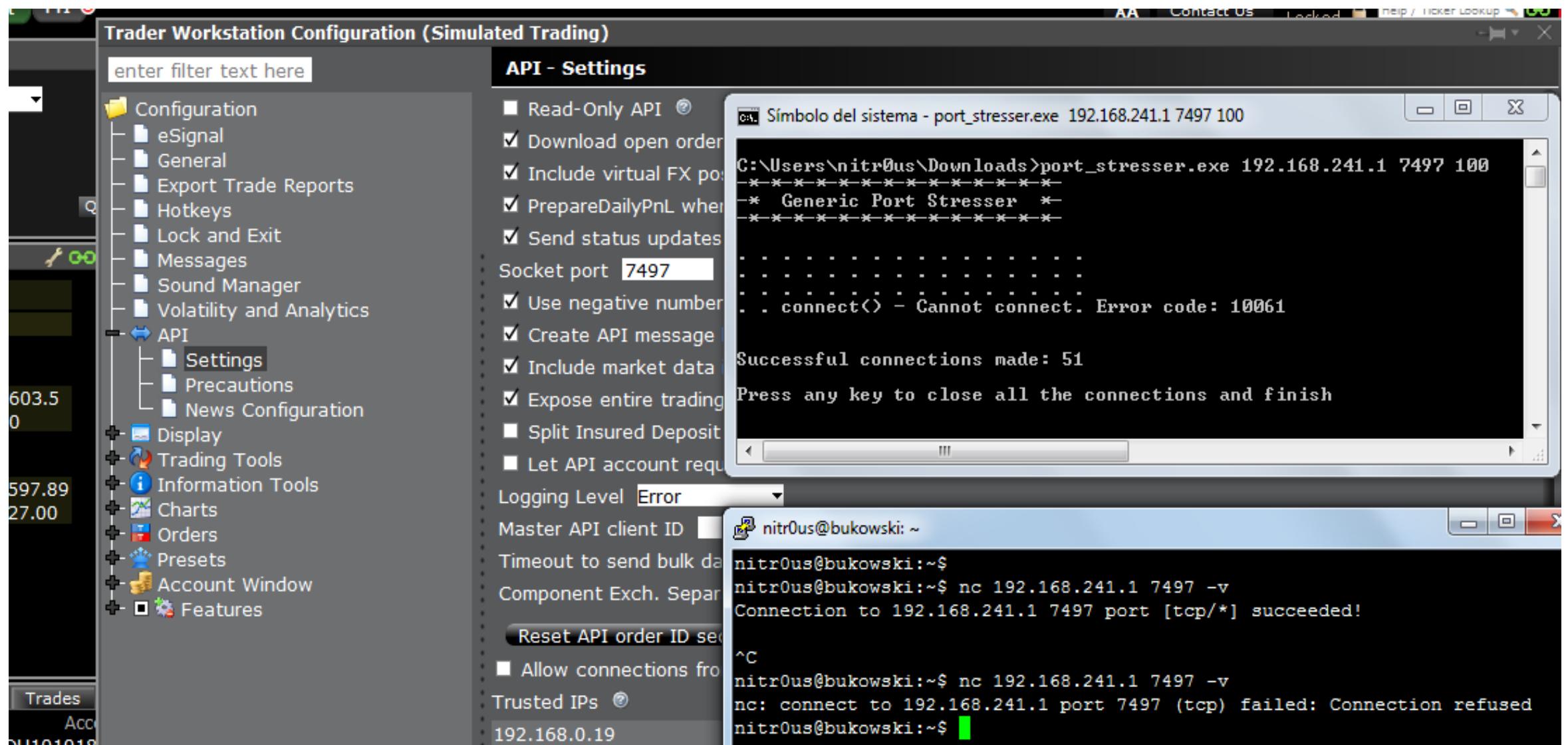
DEMO

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

Denial of Service

- 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



MetaTrader
backdoor disguised as an
Ichimoku indicator.

DEMO



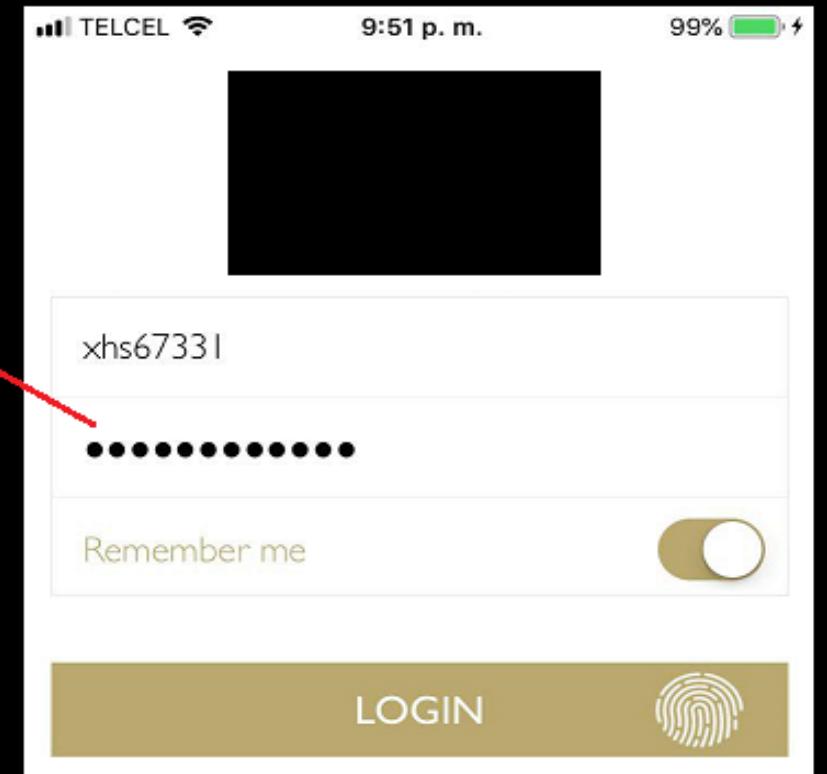
NinjaTrader
Malicious code in a chart
style.

Passwords stored unencrypted

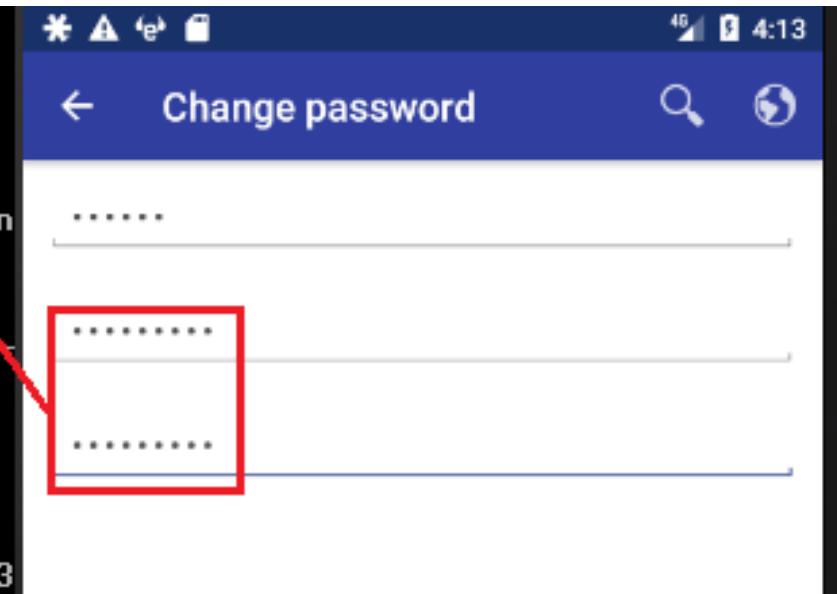
- **Passwords stored unencrypted**
 - 3 desktop applications (21%)
 - 7 mobile apps (21%)
- Stored unencrypted
 - Configuration file
 - Logs
 - File in the fs
 - Logging console
 - adb logcat
- *Log in, sell stocks, transfer money to a newly added bank account, delete this bank account, log out.*



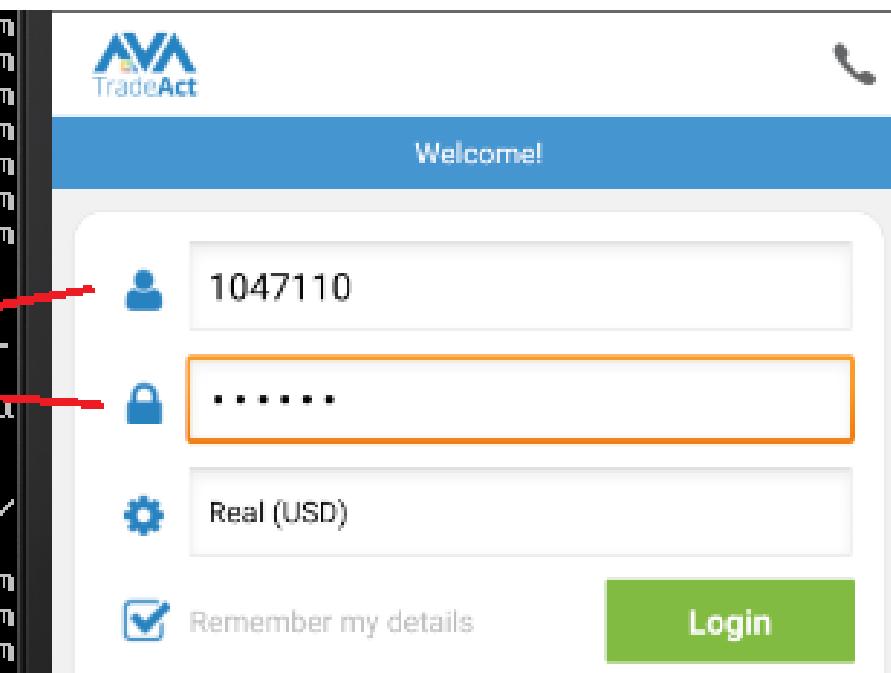
```
nitr0us@bukowski:~/ios/  $ plistutil -i Container/Library/Preferences/com.  
egrep -i "userLogin|userPassword" -A 1  
    <key>userLoginPlainText</key>  
    <string>xhs67331</string>  
--  
    <key>userPassword</key>  
    <string>rCICasboMHL38M8gME0Ix81JrMKoj7if56UN6UDzBXALTYmXrdzw014eB/L7ex3OXJFZG/LhUaAG4bczDeP  
EJvLdkxDoui9jB3yFVhlWwHs5sZShKBt1CMGVuncLyPhcbI11x0Jyq753xOSK8IJ8cR44GrorIN0z3vZxcXfh7bCq+enKuHjEvSG  
qS2TvH0Fmod8cFTKpwTdA94rzcQYR1ab1ajqATqGpYGvsPsJz/2FYJV3/qTNwNT508Q73G/famKaHkuUZEUT197r8ldjZNUR9s8/  
Xf9AcnfS5sQVjzPlIc0J0N8KFLFgHtCnR8oS9bIB8OCela+CWcDT4wG9sQ%e%q%e%q</string>  
--  
    <key>userLoginPlainText</key>  
    <string>xhs67331</string>  
    <key>userPasswordPlainText</key>  
    <string>QwertYf00b4r</string>  
--  
    <key>userLogin</key>  
    <string>uTkLGmo6PsHfIagr+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 time 739
ssDialog with keepKey = NetworkCall changePassword b3e125cb-30dc-4
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
completed, class=
gressDialog dismiss the key=NetworkCall changePassword b3e125cb-3
```



```
gralloc_ranchu: gralloc_alloc: format 1 and usage 0x900 im
AudioFlinger: mixer<0xb0103a00> throttle end: throttle time
DebugMessages: start login
ApiRec : logout()
ApiRec : Can not execute request while status is Offline.
ApiRec : login<deal.35, 1047110, PSDJK2, ...>
ApiRec : UserAgent: AvailradeHct z.3.36(85)<Android SDR pu
DataContainer: setStatus(STATUS_CONNECTING)
ApiDataContainer: doLogin<http://real16.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
```



Base64 != encryption

The terminal window displays the following command and its output:

```
nitr0us@slacker:~$ echo -n UXdlcnR5ZjAwYjRy | base64 -d
Qwertyf00b4r
```

The password "UXdlcnR5ZjAwYjRy" is highlighted with a red box. The resulting password "Qwertyf00b4r" is also highlighted with a red box.

A screenshot of a dark-themed login dialog box. It contains fields for "Username" (xxx@foo.com) and "Password". The "Password" field is highlighted with a red box. Below the fields is a "Remember Me" checkbox and a "Login" button.

```
<?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;Accou
ntCrmGuid&quot;:&quot;1759407&quot;,&quot;Currency&quot;:&quot;USD&quot;,&quot;AccountID&quot;:&quot;21
022981&quot;,&quot;ServerName&quot;:&quot;demo&quot;,&quot;AccountType&quot;:&quot;Demo&quot;}],&quot;E
mail&quot;:&quot;[REDACTED]@gmail.com&quot;,&quot;Token&quot;:&quot;iMxKHJVvR7Wdf8nvHNewdBTWBdb0j11
uswR6ekkT11414HeTSuASp0JKpwc88y5NvrDnmtPz9YuxMNsoFLNzwI9CiBnRRr4y3rJwfbdvXD0%2bdBmTIbLeVC46Bn1kSbYd9mIgR
V%2bYeyQv51vRE1h5dQG1HOjNz1ts9SHrc71BS%2b%2fDMPsJCmE7VID6C70ZxJsZevzW4P0vJeF6w1P5DCz1UYWyRGWuOFJBhsAhMX
6XHSAfcA7BI1XbHjrjKAIdvJ67E7FwWWUzRLs%3d}&quot;}</string>
    <string name=".key_crm_credentials">{&quot;credentialsTO:&quot;:{&quot;credentialsType:&quot;:{&quot;
name:&quot;REGULAR&quot;,&quot;ordinal:&quot;:0},&quot;login:&quot;[REDACTED]@gmail.com&quot;,
&quot;password:&quot;:&quot;6ynH26rP&quot;},&quot;expirationDate:&quot;:1529618798765}</string>
</map>
```

Burp Suite Professional v1.7.3 - 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">{&quot;credentialsTO:&quot;:{&quot;credentialsType:&quot;:{&quot;name:&quot;&quot;REG
</map>
```

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

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]@gmail.com> ★

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

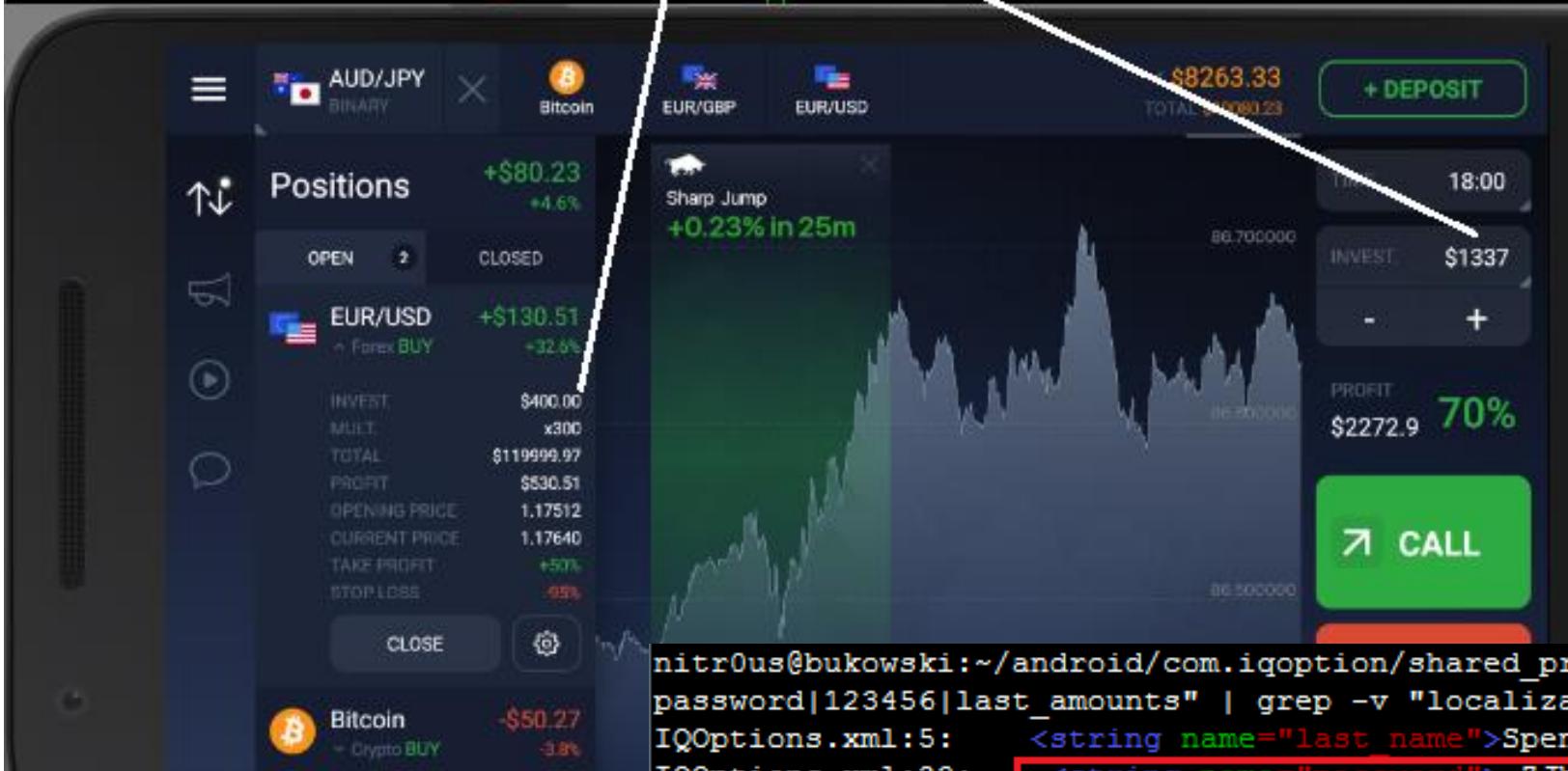
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="password">Qwertyf00</string>
    <string name="cache.url.csprodlive">live-trader-mob12.markets.com:443</string>
    <string name="last.server.address">live</string>
    <long name=".authStartTime" value="1529451161870" />
    <boolean name=".first_launch" value="false" />
    <string name="firebase_instance_token_key">d0uzkIq019M:APA91bHeZ7mvHECKjnMHrrri3Ng_uLBFzfA0p2gwL4u6jWvUA5vG5BjgLiFWqEfQZEYDh39nXxvdBluSFEqVLrY-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.m...</string>
    <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' standar...</string>
    <string key="CHART_ID" value="173873340" />&lt;string key="edit_index" value="t...true" />&lt;bundle key="0.parameters.bundle" />&lt;string key="parameters.co...quot;autoposition_mode" value="true" />&lt;string key=".fitVertical" value="false" />&lt;string key="show.indicators" value="true" />&lt;...>
```

```
bukowski:~/ios/ . . . $ sqlite3 "Container/Library/Application Support/15...
elect * from _____"
|0|0|0|0|0|0|||1||1|914347700.631725|4eb4961a8bec044e07bd42b255dfce89a181714e2aaea35124cc6|MX|Mexico|...@gmail.com|https://www. /join/5b48dc40bec71|John Spencer|MXN|1739|7ac53fdcaea9afe090910307485604a7b360f2ec2009a647bb4bc12f926e830-9426-5634-8507-eded4f8af1a7|hplist00$efX$versionX$objectsY$archiverT$top
s@bukowski:~/ios/ . . . $ [REDACTED]
```

Unlock with your PIN



```
nitr0us@bukowski:~/android/com          $ egrep -nir "      |john|spencer|Qwerty|1337"
shared_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                @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                @gmail.com</string>
app_pref_name.xml:17:   <string name="login_email">n                @gmail.com</string>
nitr0us@bukowski:~/android/com.iqoption/shared_prefs$
```

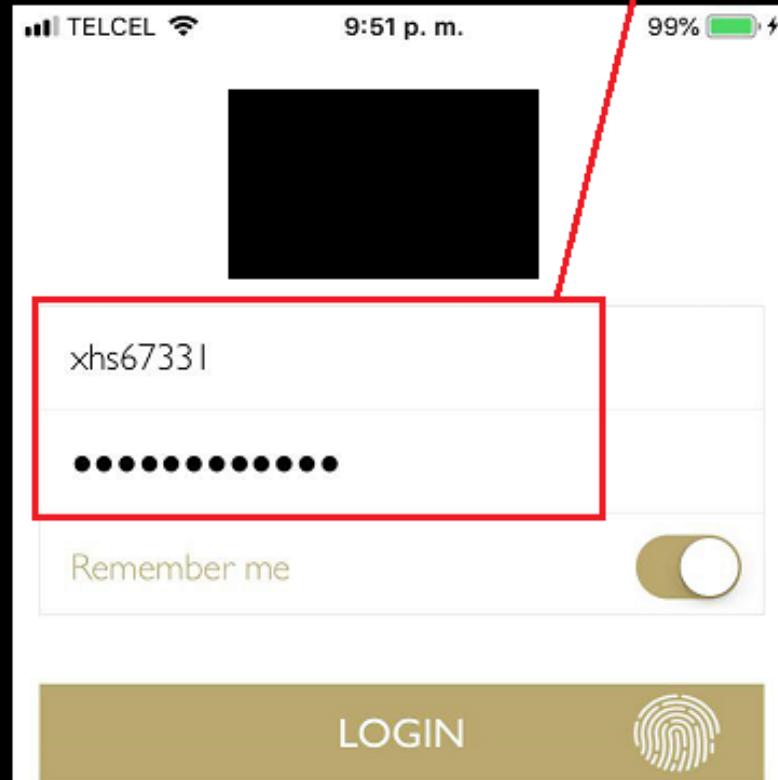


DETALLES DEL DISPOSITIVO:



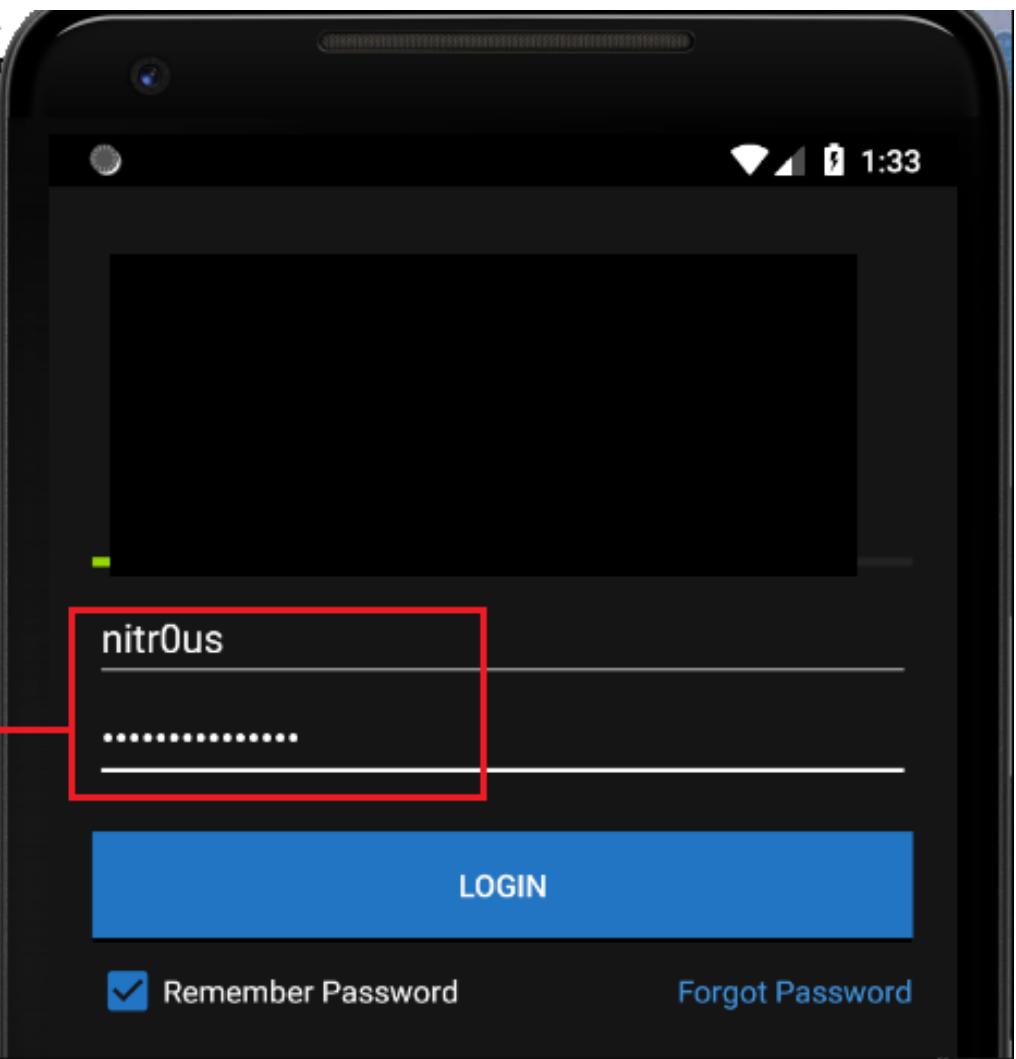
- iPhone 6 - iOS 11.4
- 18/07/2018 09:38 p. m.
- 7 copia(s) de seguridad
- DANGER (C:) (34.67 GB)
- @ [REDACTED]
- +52 (55) [REDACTED]

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



C:\ Administrador: Símbolo del sistema - adb logcat

```
07-15 01:32:55.577 1414 3454 W audio_hw_generic: Not supplying en  
only 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: eglGetCurrent: 0xd  
07-15 01:32:56.168 5640 5683 I chatty : uid=10083(  
07-15 01:32:56.208 5640 5683 D EGL_emulation: eglGetCurrent: 0xd  
07-15 01:32:56.228 5640 6755 E Volley : [264] BasicNetwork.perf  
ps://  
com/v1/user/login.json?device_version=And  
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.andr  
BasicNetwork.java:142)  
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: at com.andr  
her.java:110)
```



THIS IS NOT A BROKERAGE ACCOUNT. THIS IS A PAPER TRADING ACCOUNT FOR SIMULATED TRADING. THE MARKET DATA IS DELAYED

New Window ▾ IBot FYI ①

AA

Contact Us

Layout Locked

Help / Ticker Lookup

Order Entry

AMZN

◆ 1602.50 ◆ 1603.50 ◆
BID MID ASK

Adaptive

Option Chain



Complete your Application

Ready to Start Trading?

Experience our best price execution and generate higher

Complete

BUY SELL

QTY 100 LMT LMT PRICE 0.00 DAY advanced +

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

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
- APT

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

C:\Jts\heojhcohbmemofkedbpaiefmfjihppfadgbmajfm\tws.Sat.xml - Notepad++

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

tws.Sat.xml

```
<ESignalSettings varName="esignal" allowed="true"
username="myeSignalUsername" password="s3cr3t" host=
"CM*.esignal.com" throttlingPace="1" apiUnpacedUpdates=
"true">
<sigtext></sigtext>
<ESignalSecSettings varName="opt">
<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

X

Filter ?

1 Exces

SMA

VAL

739

399

579

395

503

338

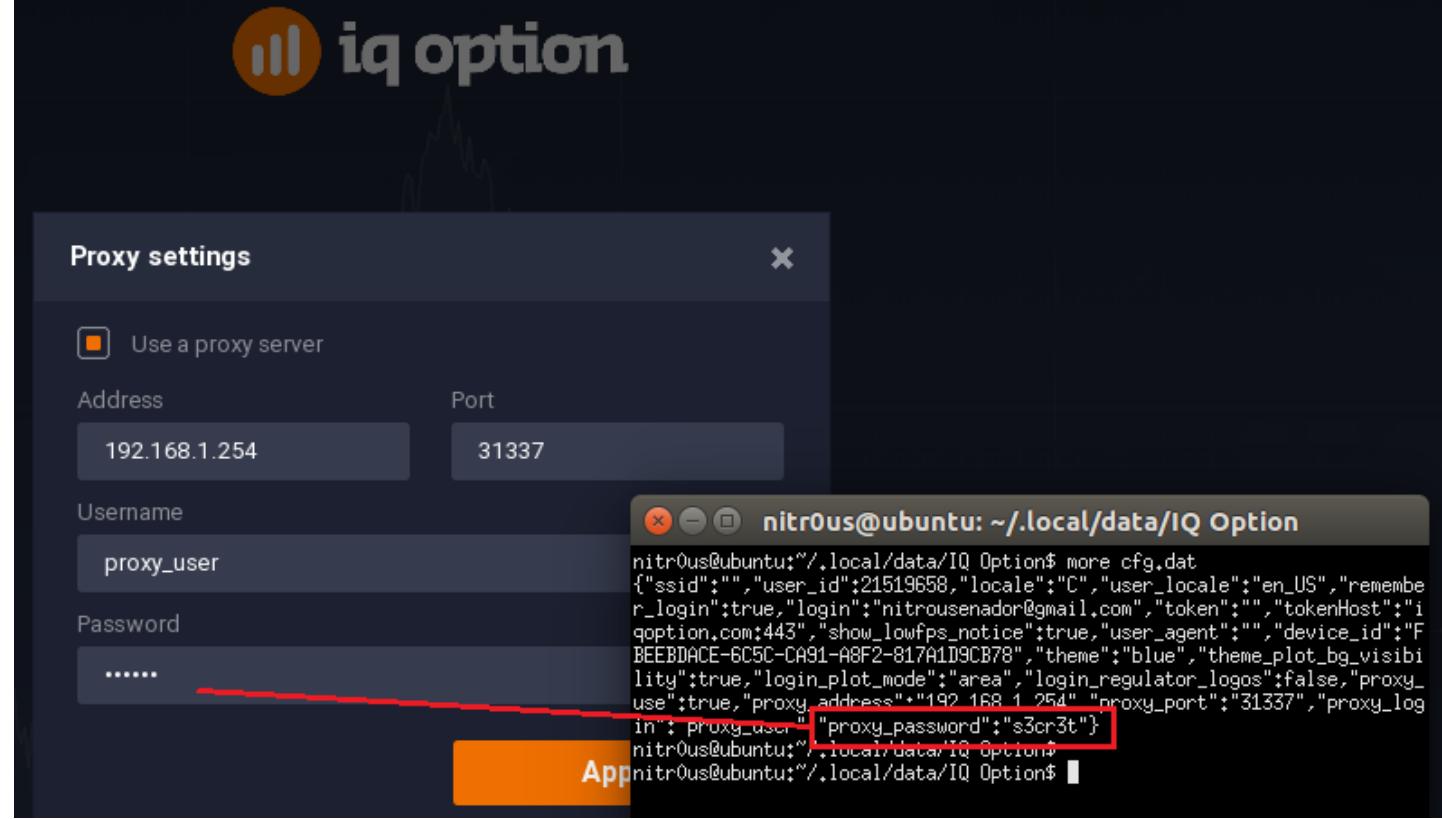
905

729

-1,024,7...

504

1,000,571

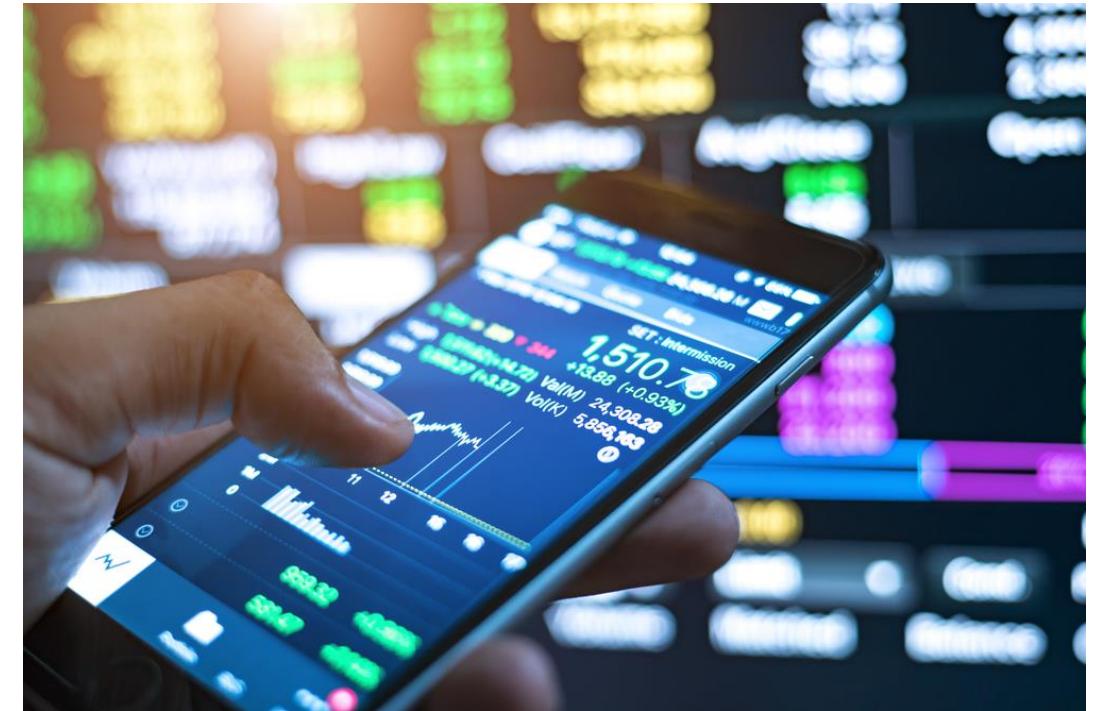


The screenshot shows the 'AvaTradeAct' application interface. On the left, there's a sidebar with 'Preview', 'Login', and 'Settings' buttons. The 'Settings' section contains 'HTTP Proxy Settings' with 'Use Proxy' checked, 'Server' (192.168.1.1), 'Port' (8080), 'Login' (myproxy), and 'Password' (redacted). Below it is the 'Alternate Configuration Server' section with 'Server' (alternate-server.mycompany.com) and 'Port' (1337). To the right, a Notepad++ window titled 'C:\Program Files (x86)\AvaTradeAct\user_loader_settings.xml' shows XML code. A red box highlights the proxy configuration block: '<proxy enabled="true" server="192.168.1.1" port="8080" login="myproxy" password="s3cr3t"/>'.

```
<?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="Z0C84X8qOEYX2lk03GuZphKUs97hhB3+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

- **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.*



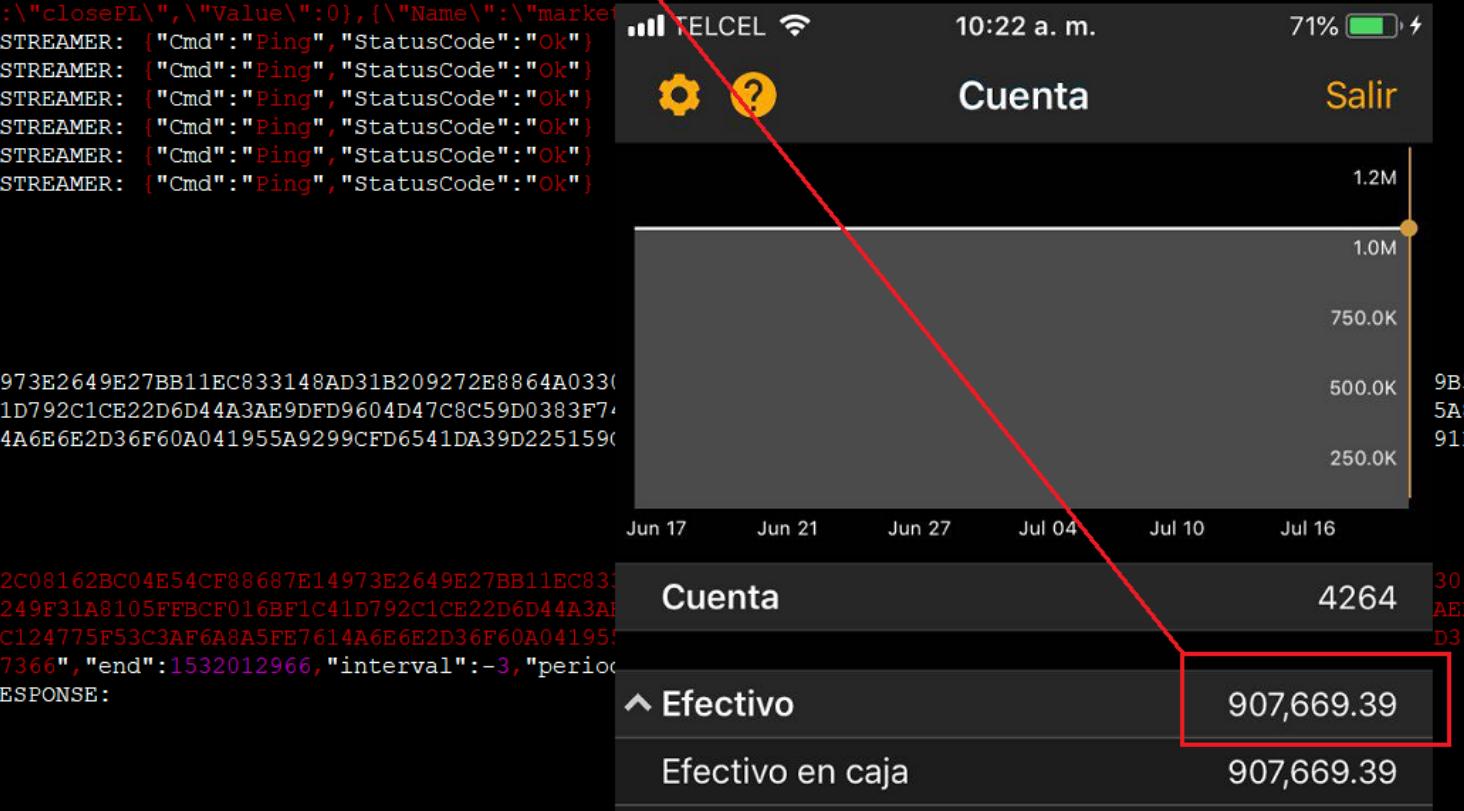
- **Trading data stored unencrypted**
 - Balances
 - Portfolio
 - Personal data
 - Buy/sell orders
 - Watchlists
 - Quoted symbols
 - Other data

INSTRUMENT	LAST	CHANGE	POSITION	P&L
AAPL NASDAQ.NMS	188.55	-0.04	1.34K	101
BAC NYSE	31.11	+0.19	1.89K	407
BRK B NYSE	200.00	+0.70	250	203
C NYSE	72.76	-0.10	726	36.3
FSLR NASDAQ.NMS	74.84	+2.06	894	1.82K
HSBC NYSE	50.27	+0.09	965	91.7
IBKR NASDAQ.NMS	78.37	-1.33	2.90K	-3.97K
ISRG NASDAQ.NMS	466.55	-1.80	1.04K	-1.81K
JPM NYSE	113.99	+0.12	576	86.4
MA NYSE	192.57	-0.78	375	266
PLNT NYSE	39.40	-1.09	15.7K	-16.82K
RY NYSE	78.87	+0.38	574	222
SNBR NASDAQ.NMS	28.46	+0.08	100	9.00

```
1g. now pending size=21; runnable=Partition
25=WFC@7051=WELLS FARGO & CO@7221=NYSE@6078
3+0.09@
4g. now pending size=22; runnable=Partition
5LR@55=FSLR@7051=FIRST SOLAR INC@7221=NASDAQ
6DW@99999999+=+2.02@
73=investors_marketplace@7261=E@7259=https://
8brokers.com/partitions@
9g. now pending size=23; runnable=Partition
055=RY@7051=ROYAL BANK OF CANADA@7221=NYSE@6079+=+0.38@
1g. now pending size=24; runnable=Partition
2C@55=BRK B@7051=BERKSHIRE HATHAWAY INC-CL
3B@99509=DW@99999999+=+0.79@
4g. now pending size=25; runnable=Partition
5PLNT@55=PLNT@7051=PLANET FITNESS INC - CL A@706509=DW@99999999=-1.10@
6g. now pending size=26; runnable=Partition
7C@55=HSBC@7051=HSBC HOLDINGS PLC-SPONS ADR@99=DW@99999999+=+0.10@
8g. now pending size=27; runnable=Partition
95=BAC@7051=BANK OF AMERICA CORP@7221=NYSE@6079+=+0.22@
1g. now pending size=28; runnable=Partition
2R@55=IBKR@7051=INTERACTIVE BROKERS GRO-CL
3B@991=DW@99999999=-1.25@
4g. now pending size=29; runnable=Partition
55=AAPL@7051=APPLE INC@7221=NASDAQ.NMS@6079+=-0.05@
6the application may be doing too much work or
7g. now pending size=30; runnable=Partition
8C@55=ISRG@7051=INTUITIVE SURGICAL INC@7221=
95.5706509=DW@99999999=-1.78@
10g. now pending size=31; runnable=Partition
115=C@7051=CITIGROUP INC@7221=NYSE@6078=OPT.
129
13g. now pending size=32; runnable=Partition
145=MA@7051=MASTERCARD INC - A@7221=NYSE@6079+=-0.75@
15g. now pending size=33; runnable=Partition
16C@55=SYMC@7051=SYMANTEC CORP@7221=NASDAQ.NM
179@99999999+=+1.87@
18g. now pending size=34; runnable=Partition
19K@7219=SSDOY@55=SSDOY@7051=SHISEIDO LTD-SPONSORED A
2076.11@6509=DW@99999999+=+5.31@
21ed pending. now pending size=35; runnable=Partition
227219=JPM@55=JPM@7051=JPMORGAN CHASE & CO@7221=NYSE@609=DW@99999999+=+0.17@
23ed pending. now pending size=36; runnable=Partition
24TK@7219=SQ@55=SQ@7051=SQUARE INC - A@7221=NYSE@6078
259=DW@99999999=-0.38@
```

```
I System.out: <liabilityExists>NO</liabilityExists>
I System.out: <singleBrkg/>
I System.out: <Funded/>
I System.out: <hasLovalAccts>NO</hasLovalAccts>
I System.out: <AssetValue>$0.00</AssetValue>
I System.out: <FmtLgrBankBalanceTs/>
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: <MarginLevel1Cd>1</MarginLevel1Cd>
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: <HccountDescType>INDIVIDUAL</HccountDescType>
I System.out: <LedgerAccountValue/>
```

Balances	
Net Assets	\$0.00
Individual Brokerage -4142	(View Details)
Net Account Value	\$0.00
Available for Withdrawal	\$0.00
Cash Purchasing Power	\$0.00
View Portfolio ▶	



```
22:%%222017-08-02T16:08:52.7757946-04:00%22%7D,%22History%22:%7B%22Items%22:%5B%5D,%22TransactionCount%22:0,%22TimeStamp%22:%222017-08-02T16:08:52.74351%22%7B%22TimeStamp%22:%222017-08-02T16:08:52.7425936-04:00%22%7D,%22Positions%22:%7B%22MoversOrHoldings%22:%5B%5D,%22Items%22:%5B%5D,%22Cash%22:0,%222017-08-02T16:08:52.7689591-04:00%22%7D,%22WsodToken%22:"XXX108_U6+zELV63gPiA4xLeHq1GHfxLrfe8EJSD3kRwe9185Y22bJNjnL/wM1K3VS2rD3/1j1eTmzzwbtXwMDK7itdsAQuoeavu0Uc", "Timestamp": "2017-08-02T16:08:52.000000000Z", "Status": 200, "Config": {"method": "GET", "transformRequest": [null], "transformResponse": [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
@07098=500@  

08-11 13:13:10.139 3098 3115 I aTws : [IN-0-0]: 35=P@6040=S@320=207@9905=509
@01-0@6119-0@7094-1442@72=1.33@76=1.34K@73=24194.35@75=2.67@6070=STK@7219=AMX@55
=AMX@7051=AMERICA MOVIL SPN ADR CL L@7221=NYSE@7039=1@6119-1@7091-15@219582@72=50
@076 5@073 1@25-300@75 2.00@6070=STK@7219=GPRO@55=GPRO@7051=GOPRO INC CLASS A@72
21=NASDAQ.NMS@7039=1@6119-2@7091-7@7222@1@72=446@76 14@73 15@131.62@75=-32.85@60
70=STK@7219=TSLA@55=TSLA@7051=TESLA INC@7221-NASDAQ.NMS@7039=1@6119-3@07094=BASE@7
3=811K@55=BASE@7158=1@6119=4@7074=USD@73=811K@55=USD@7158=16@  

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()

```

Portfolio

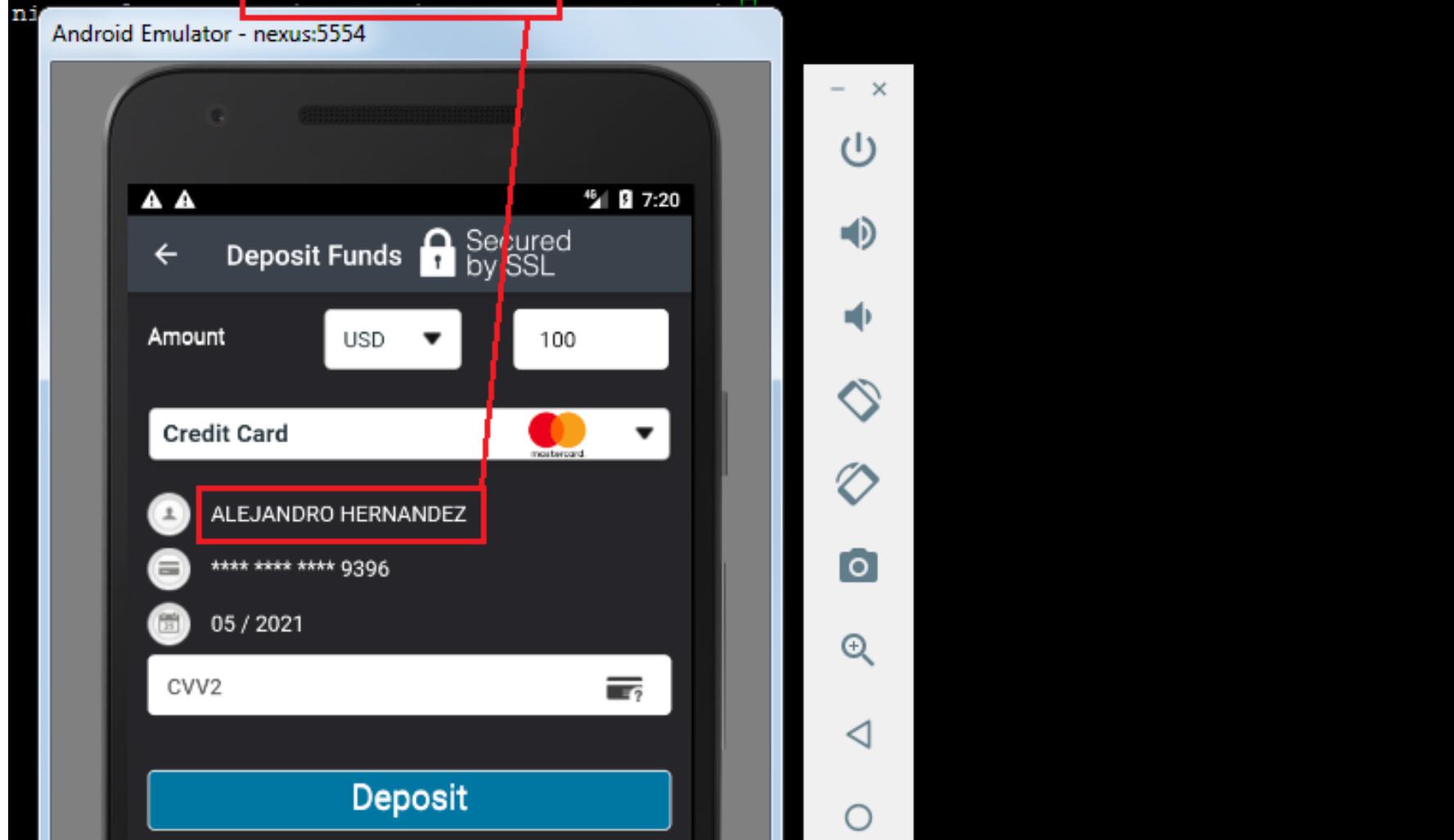
ACCOUNT	P&L	NetLiq		
DU777918	117	1M		
ExLiq	952.9K	SMA	905.8K	Unrlz
MntMgn	47.16K	BuyPwr	3.811M	Rlzd
INSTRUMENT	LAST	CHG	POS	P&L
AMX NYSE	18.12	+0.21	1.34K	34.8
GPRO NASDAQ.NMS	9.81	+0.03	500	7.50
TSLA NASDAQ.NMS	357.71	+2.31	446	74.4
TOTAL Cash	811K	(Market Value)		
USD Cash	811K	(Market Value)		

```

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"
}

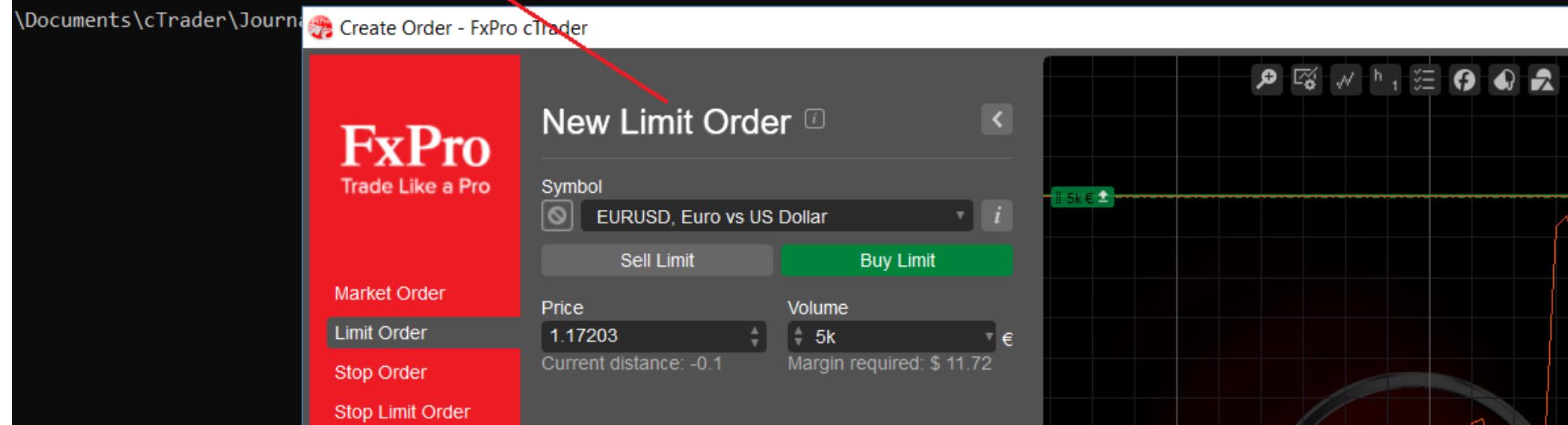
```

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



ema

```
\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 1k EURUSD (Price: 1.17203) is sent to server
:42.785 | Øå€ Limit order OID138943786 to Buy Øé% 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 | Øå€ 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 Øé% 5k EURUSD (Price: 1.17203) is sent to server
:20.775 | Øå€ Limit order OID138943789 to Buy Øé% 5k EURUSD (Price: 1.17203) is ACCEPTED (21/07/2018 23:47:20.578 UTC+0)
```



Order Entry

ISRG

462.92 463.26

Adaptive Option Chain

BUY SELL

QTY 1,337 MKT MARKET DAY advanced SUBMIT

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

L: 463.19 CH: -7.84 CH%: -1.66% 475.00

C:\Jts\dzgimyvzq\Thu.trd - Notepad++

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

Thu.audit.xml Thu.trd

```

5 35=8 SOH34=000254 SOH43=N SOH52=20180419-14:10:13 SOH11=296181529.0 SOH17=0001b25e.5
d82a94.01.01 SOH150=1 SOH20=0 SOH39=1 SOH55=ISRG SOH100=AMEX SOH207=AMEX SOH38=1337 SO
44=0.00 SOH32=100 SOH30=AMEX SOH31=463.75 SOH14=700 SOH151=637 SOH851=2 SOH6=463.75 SO
54=1 SOH37=002e9ace.00013e82.5ad81f72.0001 SOH1=D11010182 SOH167=CS SOH60=20180419-

```

D aTws : Keyboard up - don't show the submit slider
 D aTws : Keyboard up - don't show the submit slider
 D aTws : Keyboard up - don't show the submit slider
 D aTws : Keyboard up - don't show the submit slider
 I aTws : [OUT-0]: 8=FIX.4.1@9=0102@35=d@320=86@7094=76792991@54=B@1=DU777918@151=12@7228=1667831@10=121@
 I aTws : [IN-0-0]: 35=u@6040=I@
 I aTws : [IN-0-0]: 35=d@320=86@7000=1@11=955433434@7228=1667831@7108=Filled@
 I aTws : [OUT-0]: 8=FIX.4.1@9=0032@35=m@320=87@6040=S@11=955433434@10=13@
 I aTws : [main]: hiding transmitSlider. set orderId=955433434@
 I aTws : [IN-0-0]: 35=m@320=87@11=955433434@7094=26292991@65=TSLA@4=B@7219=ISLA@72@
 DU777918@7113=LIMIT@7104=357.65@14=123@7108=Filled@7110=DAY@7115=FFFF@7114=#000000@
 7099=Bought 123 Limit 357.65 DAY@6241=1@7270=0@
 E aTws : ERR [main]: Failed to update 'OE Profit Take' Time-In-Force item since '' was supported=true;capabilities=o!.. GTC;supported=true;capabilities=o!.. OPG;supported=true;
 supported=true;capabilities=o!.. GTC;supported=true;capabilities=o!.. OPG;supported=true;order
 I aTws : [main]: Failed to update 'OE Stop Loss' Time-In-Force item since '' was supported=true;capabilities=o!.. GTC;supported=true;capabilities=o!.. OPG;supported=true;order
 I aTws : [main]: hiding transmitSlider. checkOrderIsDone orderDone, Filled
 I aTws : [main]: hiding transmitSlider since OrderStatus is done, y.a\$@58af8f5
 I aTws : [main]: hiding transmitSlider since OrderStatus is done, y.a\$@58af8f5
 I aTws : [main]: hiding transmitSlider since OrderStatus is done, y.a\$@58af8f5
 I aTws : [IN-0-0]: 35=u@34=00012@52=20170811-17:59:26@6040=H@320=5385@
 I aTws : [OUT-0]: 8=FIX.4.1@9=0021@35=u@6040=h@320=5385@10=139@
 I aTws : [main]: ActivityState:@atws.activity.orders.OrderEditActivity@7fe215>.finis

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 Realized

Buy Order

TSLA NASDAQ.NMS 357.87 +2.47 +0.69% High 361.26 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: 131.564 ⓘ 0.0

Price PIPS

132

Take Profit

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 Close Window

Submit

79.log

2018-07-17 23:31:20.211 -0500 I [AWT-EventQueue-0] Buy/Sell window submitted
: {} indicates disabled fields

[== Market Order - EUR/JPY ==]
|Market Order|
() SELL (o) BUY
Market [EUR/JPY]
Rate 131.564
(o) Price () PIPS
[x] Take Profit
[] Stop Loss
[] Trailing Stop
() Lower Bound
() Upper Bound

Units Available: 2,130,498
1 PIP = 0.12 USD
Take Profit: 5.16 USD / 43.6 PIPS
Stop Loss: 0.00 USD / 0.0 PIPS
Trade value: 1,556.79 USD
Margin used: 62.27 USD
[] Keep open

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](https://[REDACTED].com/v3/accounts/101-001-8050485-001/orders)
HTTP/1.1

2018-07-17 23:31:20.327 -0500 I [SwingWorker-pool-4298289-thread-10]
response code: 201

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":}

Realtime Data: \$DJI 25013.29 +298.20 (+1.21%) SCOMPX 7394.04 +39.70 (+0.54%) C:\Users\nitr0us\AppData\Roaming\Charles Schwab\StreetSmart Edge\417756\Settings\settings.xml - No...

Watch List

#	Symbol	News	Last T
4	NFLX		33
5	AMX		1
6	HACK		3
7	LOCO		1
8	AAPL		16
9	TSLA		28
10	PLNT		4
11	DOCU		4
12	ISRG		46

BA Go 363.92 ▲ +12.69 (3) Extended Hours: 364.15 ▲ +0.230 (0.06%) BA : 20 Periods : 15 Minute

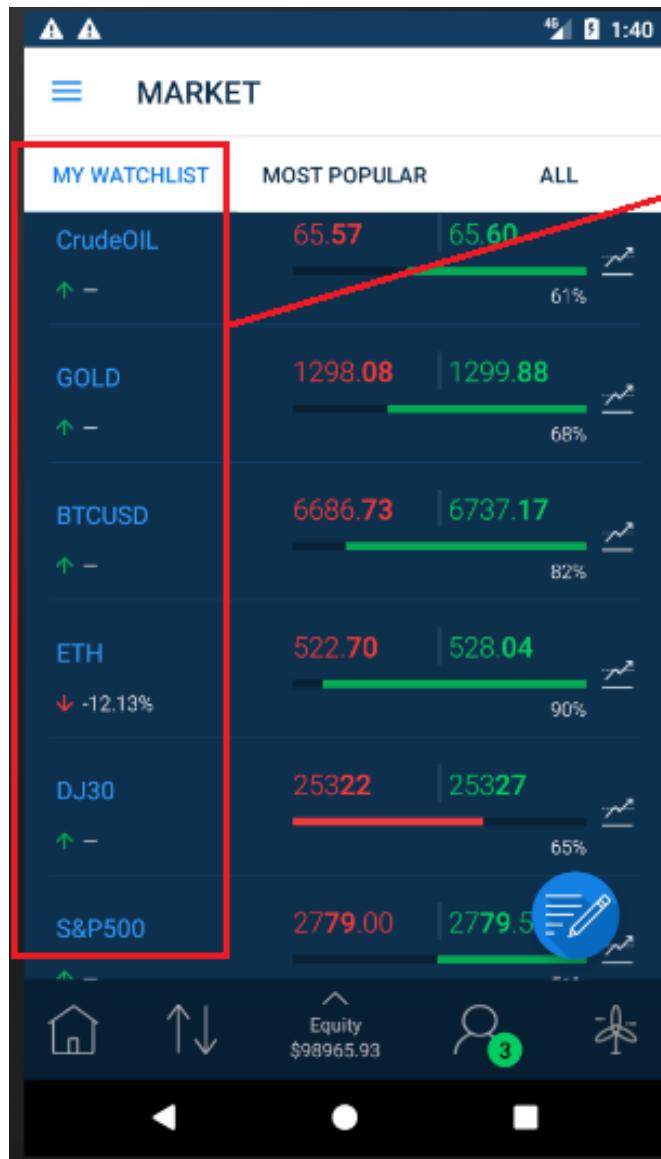
Hide: Orders Positions 20 Periods : 15 Minute BA 11:00 12:00 13:00 14:00 15:00 Date Quick Jumps ▾

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

VendorTools.xml settings.xml exceptions.SSEdgeLog NCL.txt Screener.txt gics.txt PredefinedScreen...

```
p2:type="q2:guid">00000000-0000-0000-000000000000
</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><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">00000000-0000-0000-000000000000
</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><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">00000000-0000-0000-000000000000
</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><item><key>Name
</key><value><anyType p2:type="q1:string">ISRG
</anyType></value></item><item><key>Index</key><value><anyType p2:type=
"q1:int">11</anyType></value></item><item><key>Id</key><value><anyType
p2:type="q2:guid">00000000-0000-0000-000000000000
</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
</anyType></value></item>
```

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&amp;P500;;NASDAQ100;;DAX30;;#APPLE;;#GOOG
LE;;USDMXN;;BTCEUR;;BTCJPY;;</string>
    <string name=".chart_state">&lt;?xml version='1.0' encoding='UTF-8' standa
lone='yes' ?&gt;&lt;bundle key="root"&gt;&lt;string key="CHART_
ID" value="60147996"/&gt;&lt;string key="edit_index" value="-1" /&gt;&lt;string key="show.tips" value="true" /&gt;&lt;string key="parameters.bundle" /&gt;&lt;string key="parameters.count" value="0" /&gt;&lt;bundle key=".parameters" /&gt;&lt;string key="autoposition_mode" value="true" /&gt;&lt;string key=".fitVertical" value="false" /&gt;&lt;string key=".showPortfolio" value="false" /&gt;&lt;string key=".show.indicators" value="true" /&gt;&lt;string key="selected_instrument" value="#AT&amp;T" /&gt;&lt;string key="0.fullname" value="&quot;&quot; /&gt;&lt;string key="0.name.local" value="&quot;&quot; /&gt;&lt;string key=".study_item_mode" value="0" /&gt;&lt;string key="last_visible_candle" value="2147483647" /&gt;&lt;bundle key=".selectedStudy" /&gt;&lt;string key="size" value="0" /&gt;&lt;bundle key="show.legend" /&gt;&lt;string key="type" value="1" /&gt;&lt;string key="0 fullname.local" value="&quot;&quot; /&gt;&lt;string key="autoscale_mode" value="true" /&gt;&lt;string key="0.enabled" value="true" /&gt;&lt;string key="compact" value="false" /&gt;&lt;string key="0.name" value="&quot;&quot; /&gt;&lt;bundle key="0.plots.bundle" /&gt;&lt;string key="plots.count" value="0" /&gt;&lt;bundle key="data_state" /&gt;&lt;string key="candleWidth" value="1" /&gt;&lt;/bundle></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.etrade.mobilepro.activity/WatchListActivity
I System.out: Before calling service url /e/t/mobile/GetWatchListEntries
I System.out: response is <GetWatchListEntriesResponse xmlns=>
<Location="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>NASDAQ</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>NASDAQ</ExchangeCode>
I System.out: <EntryId>3344137001</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>SPY</Symbol>
I System.out: <Display_Symbol>SPY</Display_Symbol>
```

Watch Lists

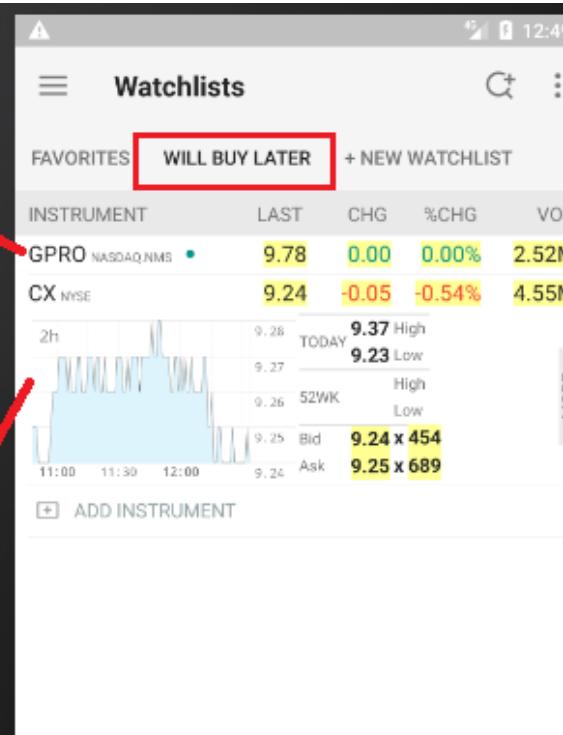
Select WatchList
POTENTIAL INVESTMENTS

POTENTIAL INVESTMENTS	+	edit		
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,

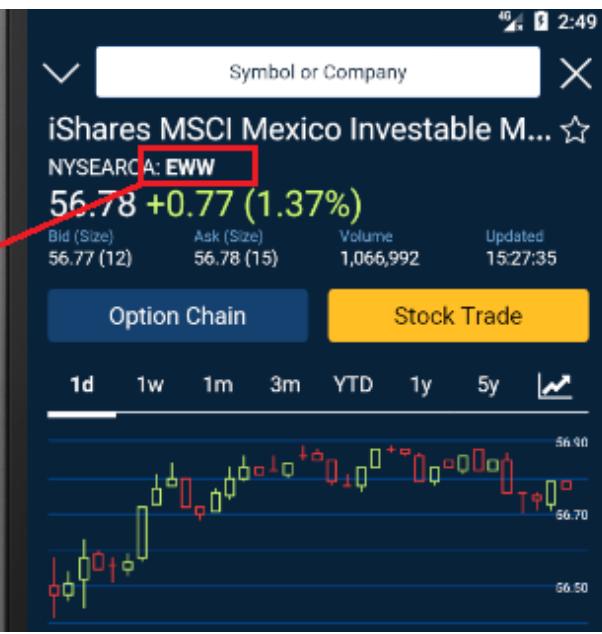
```
nitr0us@bukowski:~/android/com.firstrade.android$ strings app
Cache/99c50ebdbfed13b7_0 | grep symbol
t@https://api3x.firstrade.com/private/getfav/"statusCode":200
e:"Normal","result":{"list_id":1,"name":"Mobile Favorites","hlist_id":1186971,"sec_type":1,"symbol":"B","quantity":0,"last":60.01,"ask":60.01,"vol":285947,"change":1.32,"change_percent":2.26,"unit_cost":0,"cost":0,"gain_amount":0,"gain_percent":0,"bid":59.24,"high":60.24,"low":59.31,"close_price":58.68,"update_time":"00:00:00","hlist_id":1186905,"sec_type":1,"symbol":"EWW","quantity":0,"last":56.69,"ask":56.69,"vol":1147548,"change":0.67,"change_percent":1.18,"unit_cost":0,"cost":0,"gain_amount":0,"gain_percent":0,"size":14,"high":56.89,"low":56.41,"close_price":56.01,"update_time":00:00:00}, {"watchlist_id":1186914,"sec_type":1,"symbol":"GRBMF","quantity":0,"bid":2.45,"ask":2.49,"vol":1800,"change":0.06,"change_percent":3.33,"amount":0,"unit_cost":0,"cost":0,"gain_amount":0,"gain_percent":0,"asksize":100,"high":2.5,"low":2.48,"close_price":2.42,"update_time":00:00:00}, {"watchlist_id":1186926,"sec_type":1,"symbol":"SPY","quantity":6,"bid":246.6,"ask":246.61,"vol":51302492,"change":2.47,"change_percent":0.1%
```

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

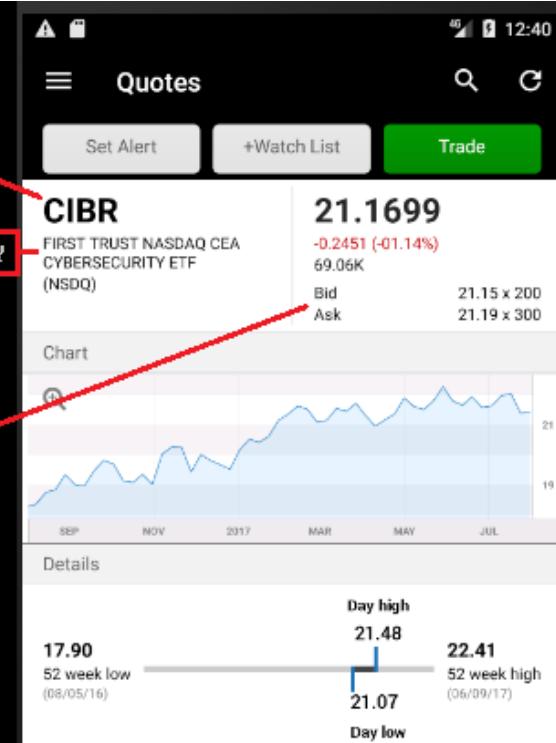
```
[OUT-0]: 8=FIX.4.109=0060035=w@320=52@7027=0@7094=158249582@7131=2h@9920
[IN-0-0]: 35=w@6119=52@320=52@55=GPRO@58=GOPRO INC-CLASS A@127=100@7116
64@1;964@2;964@3;962@4;962@5;964@6;964@7;964@8;964@10;964@11;965@12
965@21;964@22;966@23;965@24;966@25;966@26;968@27;967@28;968@29;967@30;969
99;970@40;970@41;971@42;971@43;971@44;971@45;972@46;970@47;972@48;971@49;
76@58;975@59;975@60;975@61;975@62;976@63;976@64;975@65;975@66;975@67;975@68;
981@77;981@78;981@79;983@80;983@81;983@82;982@83;982@84;982@85;980@86;9
95@979@96;979@97;979@98;981@99;980@100;979@101;980@102;980@103;979@104;
0@7213=1@7214=2@7233=2@]
[IN-0-0]: 35=w ChartData 38375662 : Can pan back: true ticks:106 max:150
[IN-0-0]: 35=w TimeSeriesManager: Server id set:52
[OUT-0]: 8=FIX.4.109=0085@35=I@320=53@1=DU777918@7094=158249582@6119=Q16
[ WorkerThread]: 35=w TimeSeriesManager: processor removed unsubscribe T
y[key=158249582:2h:::c/zt:::fx_p_off], m_serverId=52, m_reqId=52] total
[ WorkerThread]: 35=w TimeSeriesManager: Clear
[OUT-0]: 8=FIX.4.109=0012@35=w@320=54@10=1770
requesting -1 chart bars; isPan=false; TimeSeriesKey[key=6257:2h:::c/zt:::fx_p_off]
[ WorkerThread]: 35=w TimeSeriesManager: setKeyData reqId:55 key:TimeSer
[OUT-0]: 8=FIX.4.109=0080@35=I@320=56@1=DU777918@7094=6257@6119=Q17@7091
[ WorkerThread]: 35=w TimeSeriesManager: Added processor for TimeSeriesP
@2h:::c/zt:::fx_p_off], m_serverId=null, m_reqId=55]
[OUT-0]: 8=FIX.4.109=0055@35=w@320=55@7027=0@7094=6257@7131=2h@9920=10@1
[ WorkerThread]: 35=w TimeSeriesManager: Subscribe response processor c
[IN-0-0]: 35=w@6119=55@320=55@55=CEMEX SAB-SPONS ADR PART CERO@122
9@925@0;925@1;925@2;924@3;924@4;924@5;924@6;924@7;925@8;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
```



```
xpected exception: java.io.WriteAbortedException: writing aborted  
call_determinedVisibility() - never saw a connection for the pi  
javascript_dialog_manager.cc(68) [Not implemented reached in vir  
ndingDialogs<content::WebContents*>  
call_determinedVisibility() - never saw a connection for the pi  
javascript_dialog_manager.cc(68) [Not implemented reached in vir  
ndingDialogs<content::WebContents*>  
>] "Failed to decode downloaded font: file:///android_asset/www/  
le:///android_asset/www/src/charts/index.html?symbol=EWW (0)  
>] "OTS parsing error: invalid version tag", source: file:///and  
xpected exception: java.io.WriteAbortedException: writing aborted  
xpected exception: java.io.WriteAbortedException: writing aborted  
xpected 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
```

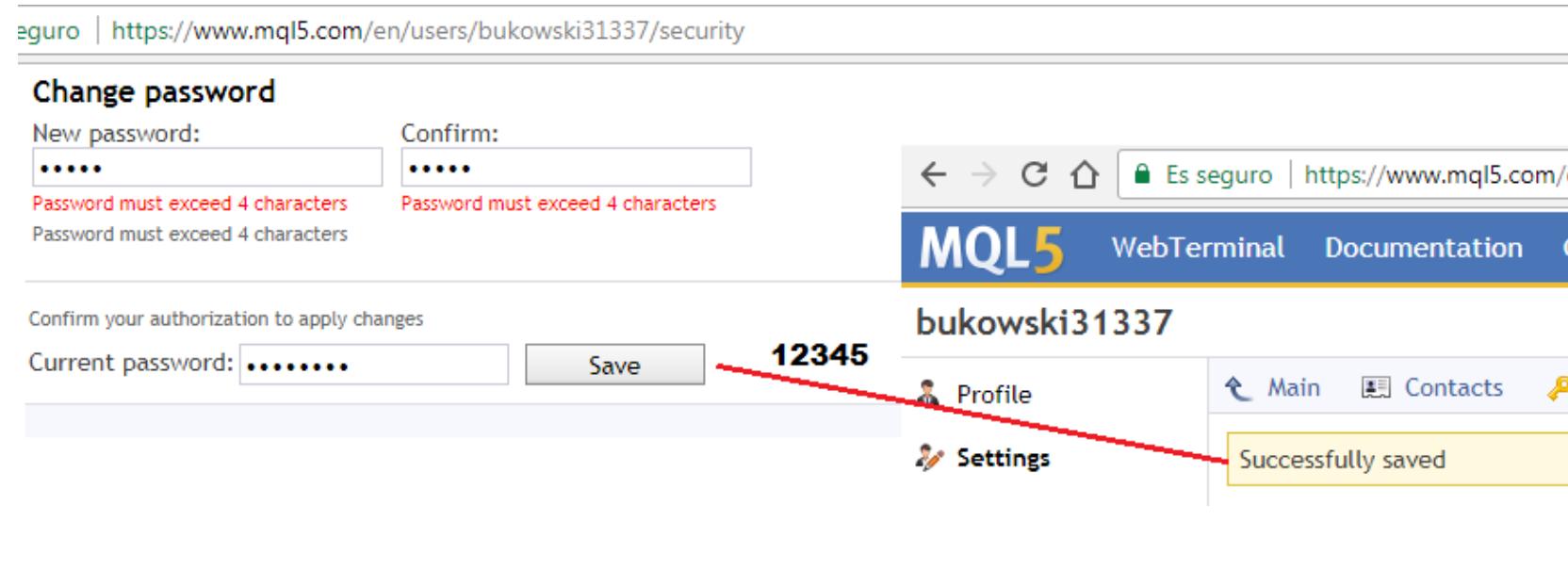


```
I System.out: <Quote>  
I System.out: <Symbol>CIBR</Symbol>  
I System.out: <ProductType>EQ</ProductType>  
I System.out: <ExchangeCode>NASDAQ</ExchangeCode>  
I System.out: <ExchangeName>NASDAQ NM</ExchangeName>  
I System.out: <ExchangeDesc/>  
I System.out: <TypeName>Equity</TypeName>  
I System.out: <TypeDesc/>  
I System.out: <Currency>USD</Currency>  
I System.out: <ProdStatus>1</ProdStatus>  
I System.out: <ProdSvcRet>0</ProdSvcRet>  
I System.out: <SymbolDesc>FIRST TRUST NASDAQ CEA CYBERSECURITY  
<Low>21.07</Low>  
I System.out: <FastMktFlag>0</FastMktFlag>  
I System.out: <NextEarningsDate>0/0/0</NextEarningsDate>  
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>69,012</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>
```



Weak password policies

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



The image contains three screenshots. The top-left shows a 'Change password' form on mql5.com where a user can set a password as short as '12345'. The bottom-left shows a user profile on MQL5 with a password '12345' highlighted by a red arrow. The right screenshot shows a mobile login screen for Plus500 where a user tried to log in with a password longer than 12 characters, receiving an error message.

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

Change password

New password: Confirm:

Password must exceed 4 characters
Password must exceed 4 characters
Password must exceed 4 characters

Confirm your authorization to apply changes

Current password: Save

12345

MQL5 WebTerminal Documentation

bukowski31337

Profile Main Contacts 

Settings Successfully saved

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

Plus500 World's Trading Machine

Registered User Login

Money Demo

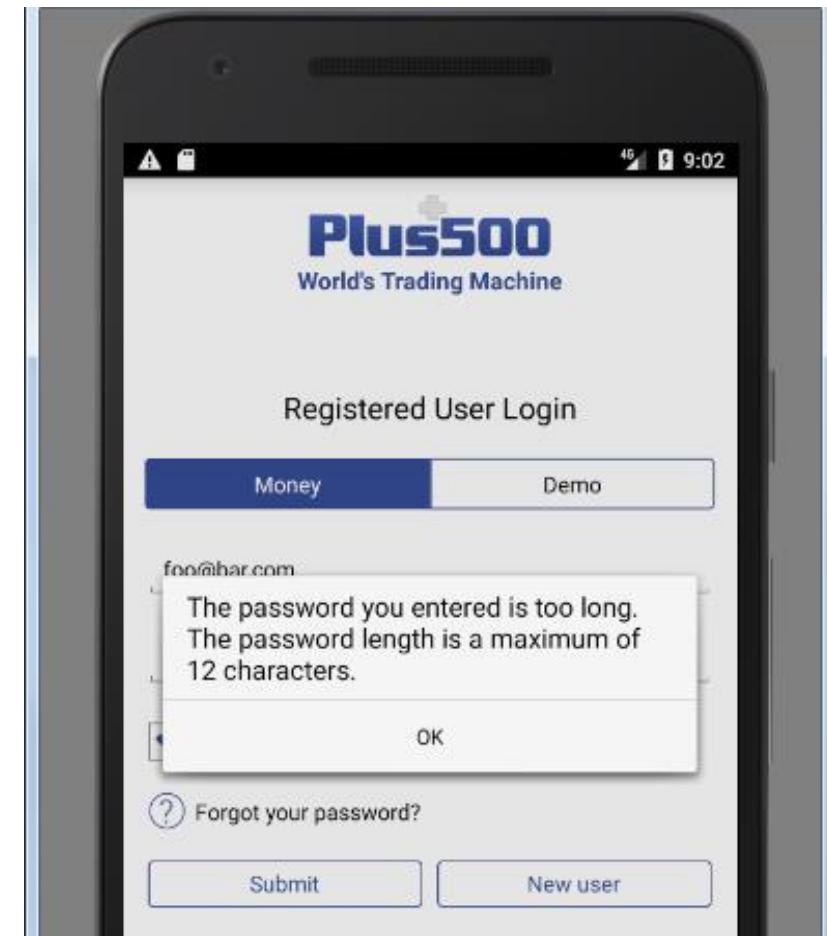
foo@bar.com

The password you entered is too long.
The password length is a maximum of
12 characters.

OK

Forgot your password?

Submit New user



Weak password policies

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



Change Password

Any questions about how to set up personal data?

Visit our [Help Center](#)



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=----WebKitFormBoundaryLNCerL0P16HxOsoS
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=GAI.2.980530117.1522723886; _gat=GAI.2.1599770701.1522723886;
landing=iqoption.com;
red_test_ab=(#22random_id#22:#22F832FD49-F1C7-E462-45SD-A4C747D8EC62#22#2C#22group#22:1); _uet94f963e7; _ym_id=1522723892832780991; lang=en_US;
pll_language=en; _ym_isad=2; _ym_visorc_22669009=w;
ssid=f763c78d630alaf9d94821cd82431772;
_uat=c9c64e071d2853bc7906c017a231adlcc46ab630; platform=15; is_regulated=0
-----WebKitFormBoundaryLNCerL0P16HxOsoS
Content-Disposition: form-data; name="current_password"
Qwertyf00b4r
-----WebKitFormBoundaryLNCerL0P16HxOsoS
Content-Disposition: form-data; name="password"
123456
-----WebKitFormBoundaryLNCerL0P16HxOsoS
```

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

Enter your old password

.....

Cancel

Save

Enter a new password

.....



!

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)

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: __utat=c9c64e071d2853bc7906c017a231adlcc46ab630; path=/
Set-Cookie: ssid=69938bd98d5db64728c9e7e0eca2accl; expires=Thu, 03-May-2018 02:56:46 GMT;
Max-Age=2592000; path=/; domain=.iqoption.com
Set-Cookie: ssid=69938bd98d5db64728c9e7e0eca2accl; expires=Thu, 03-May-2018 02:56:46 GMT;
Max-Age=2592000; path=/; domain=iq-option.com
Set-Cookie: ssid=69938bd98d5db64728c9e7e0eca2accl; 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}

MARKETS.COM Deposit and Start Trading English

SETTINGS

Customer Info

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.

Original request

Edited request

Response

Raw Headers Hex JSON Decoder

g6092921_24.group24=S1529523710.a4d2da75b7; lc_window_state.group24=minimized; incap_ses_978_756=VTExoJqVS3m5fbubBkrYrGGuKlsAAAAAQUIPAAAAAAp fj9e5r/sfcWfcIIrFWsz; incap_ses_979_1087756=E0BFCZMN6NUQIDV%3A20180620%3A9%7CBZVR4NSSBABPMPXBZNV7H%3A20180620%3A9%7C7EGFWRF2BZBEHSZMKFBEJ g6092921_27.group27=S1529523815.900924c9af; visid_incap_1204500=fyy9YfbssNCghflfQSP38CquK1sAA YN1MZWgaQbD3gWHBEjwAAAADtuHqBXf9acZeis47pww05; incap_ses_978_1204500=PMX9exh5jkSGwaSJ46SDWqu

hashedPassword=60b49a6cae fec54a3e9661b1145fa476&oldPassword=Qwertyf00b4r&newPassword=123

Used Margin: \$0.00

Real Account

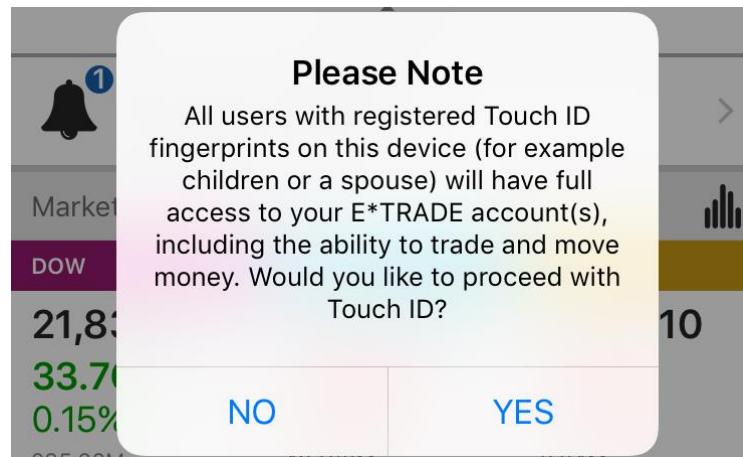
Profit / Loss \$0.00

Save Changes

Changes saved

Authentication

- 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:



Auth Token as a URL Parameter to the Browser

- 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

IQ Option

1:40 PM

PRACTICE ACCOUNT \$••••• TOTAL: HIDDEN

Deposit

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

Portfolio ACTIVE PENDING

All Positions

CURRENT PROFIT As a Percentage +\$865.72 +65%

INVESTMENT \$1,338.67

13:39 Bitcoin 22 Aug 2 Crypto +\$865.75 +65%

PUT 50%

John Spencer@gmail.com Change Photo Personal Data

Mexico Date registered 15 Aug 2017

+ Deposit \$ Withdraw Funds OTN Tokens Contact Support Transactions History Trading History

5:42

Count 337 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;|212:0;1.0|223:32; _!?!?;~ .%?": [] ???"???"<>|3843%4%6%?3502/:::/0|224:4;high| -schedulerPrefs 0001,2 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/fi ni.ja -appdir /usr/lib/firefox/browser 26268 true tab"
New Process: "/usr/lib/firefox/firefox https://auth.iqoption.com/api/v1.0/login/token?q=MjE1MTk2NTI8MzFlNjY2NjhYmZmNWI2ZWJmMTcxZjImNThiMzNkMTJhZjcxMDE4nOGEyMGFhY2I2NzlkZjExMTYzZWE5MDE1ZGI0Yzg3MGZiYzE2MThjNTEyNjNhODMzYTQ1MjRlMWnjY2M2YWR1MzY4NmRiYWJmMDM4YTh8aHR0cHM6Ly9pcW9wdGlvbi5jb206NDQzL3Byb2ZpbGU%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

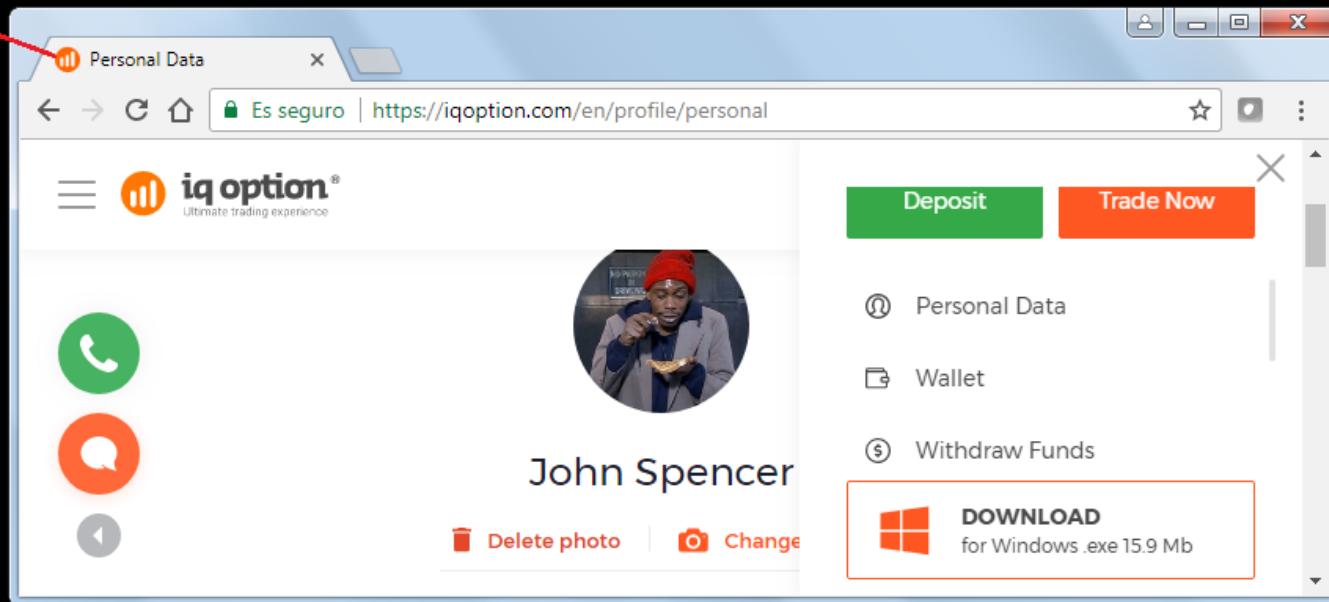
iq option® Ultimate trading experience

Deposit Trade Now

John Spencer

Personal Data Wallet Withdraw Funds

DOWNLOAD for Windows .exe 15.9 Mb



Screenshot illustrating a network analysis tool showing multiple Firefox processes running simultaneously, each interacting with the Interactive Brokers LLC [US] website.

The taskbar at the top shows several open browser windows:

- cmd.exe
- tws.exe
- firefox.exe
- firefox.exe
- firefox.exe
- firefox.exe
- firefox.exe

A red box highlights the URL in the address bar of the main browser window:

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

The browser interface displays the Interactive Brokers account management page. The URL is also visible in the status bar at the bottom of the browser window.

Key elements of the page include:

- Navigation menu: Trade, Reports, Manage Account (highlighted), Support, Logout.
- Activity section: Trade Confirmations, Tax.
- Statements section: Flex Queries, Models, Batch Reports.
- Content area: Not Available (under Activity), May 21, 2018 12:00 PM EDT (under Statements).
- Webinar information: 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.
- Margin requirements: Current Margin Requirements (USD) table.

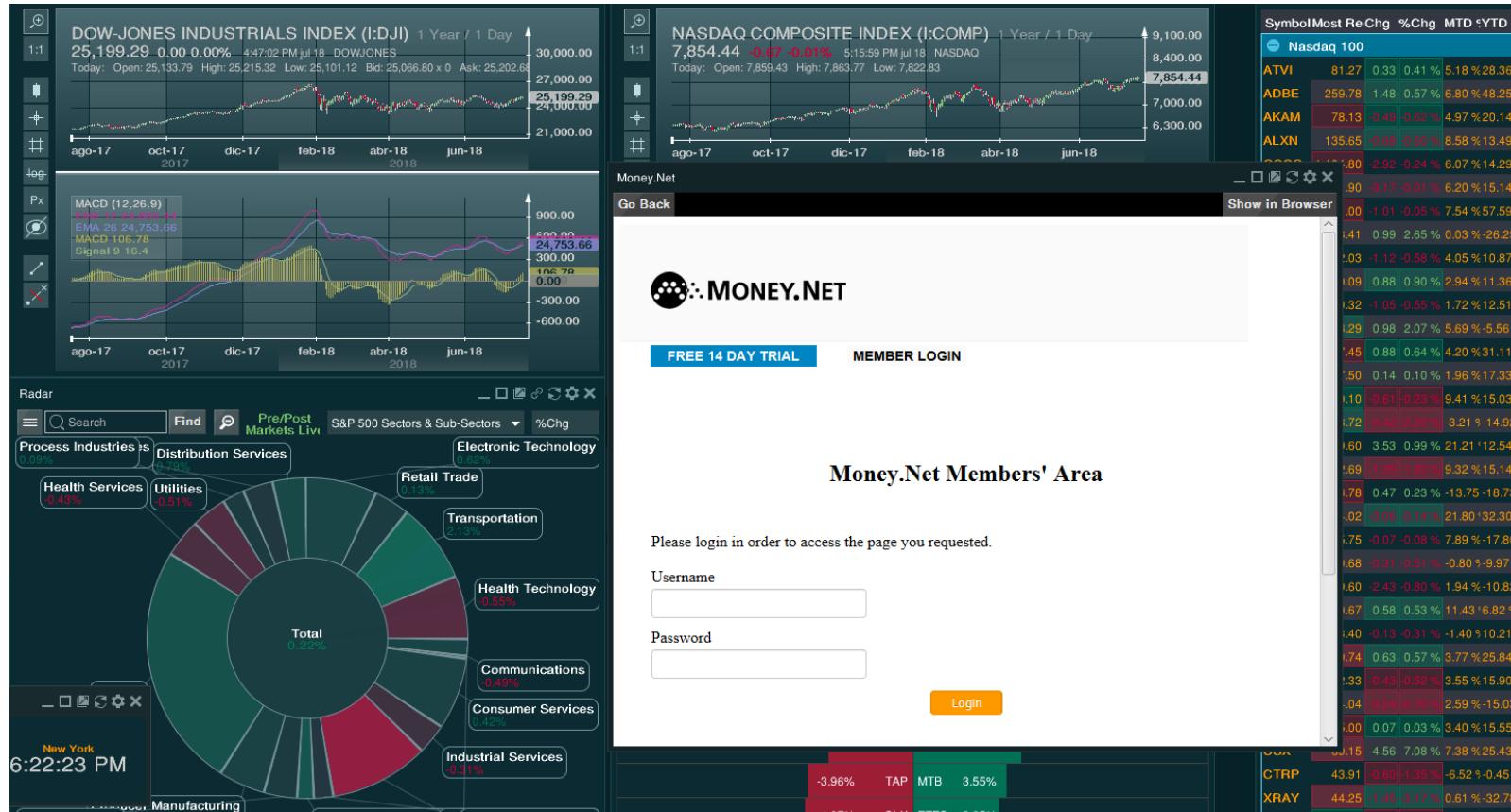
DEMO

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

Auth Token as a URL Parameter to the Browser

#BHUSA

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



Session still valid after logout

#BHUSA

- 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

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?](#)

Response

[Raw](#) [Headers](#) [Hex](#) [HTML](#) [Render](#) [Last refresh](#) March 02, 2018 5:19 PM ET

Balances

Account:

Individual Brokerage -2213

GO

Show

Previous Close

Refresh

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

Did Set Cash Available for Withdrawal

\$0.00

Net Cash Balance

\$0.00

Show Detailed Balances

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



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*****

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,  
        "isAllBrkrgAccntRequest": 0,  
        "settledCash": 0,  
        "overnightMrgnReserveForOpenOrders": 0,  
        "isManagedAccount": null,  
        "nonMrgnPurPowerAfterOrderReserve": 0,  
        "cashAvlForWithdrawl": 0,  
        "daysGainRealizedVal": 0,  
        "cashPurchasingPower": 0,  
        "contibutionsPrevYear": 0,  
        "intradayMrgnPurPowerAfterOrderReserve": 0,  
        "overnightNonMrgnPurPowerBeforeOrderReserve": 0,  
        "mrgnPurPowerBeforeOrderReserve": 0,  
        "mrgnPurPowerAfterOrderReserve": 0  
    }  
}
```

User ID

or Password?

Log on

```
"isMargin": false,  
"role": "PRI",  
"accountShortName": "Individual Brokerage [REDACTED]",  
"futuresEligible": false,  
"accountName": "",  
"dtStatusCd": "1",  
"marginLevelCd": "1",  
"accountDesc": "Individual Brokerage",  
"accountType": "INDIVIDUAL",  
"optionLevelCd": "2",  
"institutionType": "ADP",  
"tcpEligible": "2",  
"accountNumber": "[REDACTED]",  
"institutionNo": "[REDACTED]",  
"benfPermission": "2",  
"accountKey": "go7jL2mKKe4qKIH4Bai9V1TVVg0a0jdfTqTN0FJsl",  
"futuresInProgress": false,  
"typeIRA": false,
```

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-f1f3f84135a6
Origin: https://client.schwab.com
Authorization: Bearer
IO.b2F1dGgyLmJkYy5zY2h3YWlUY29t.-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?



earn more about
professional trust
management >

Request

Log Out Successful

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

Log In

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=4911C4A04EFC633642879217415535D~uwmVm2xoM4tHM5gwV4cGZxCzxFjaC52x7Krt1
QLKcz229BIZCVnIc6RCaIDBwS5cqvBhKJT03GpfrcTzyE/a5830q5vnfw0iNvc6U+ioc5mte8rBH
mtRYUMVoDMNd7KACJ28GKeuT2/XvA/D8ErxCqvtf8L4QcJTTvWVILpwN+MWVJrbgXn4XoqkrH7mT
ZM+p6gtJwQ9ySzitssAaJyuXCoxxkhx3eLIOXZ6d+DfmPB2AUjMEQw8jXU4AQWudN0mFRA97embHL
4V840cDScLGzw==;
mbox=session#d790fff226e94e31815e9ff8a411acad#1523421549|PC#d790fff226e94e31
815e9ff8a411acad.28_68#1586664065;
ak_bmsc=B9CD8DC72D4E812499BAB5D58E9E2CC642ABE160232E00007B88CD5A2421D936~p1B
D1seRDgZRMWzp+nimizoR20vL71VN+AT7b4tm09t0h02sgULpFSYUAf6By9yAOp/MND81m7Si+Ri
X2XGNExYK78RegBlaUS3RkbbJzpgDXymmmXbUVySVKph3TldeIe4yUrgclAeU7Vr3isn52KW811Hv
KSyptPNWv2UU4aGBnxLeCC1UA0liH5NChP9Bs7Tt9di+yORlpZo33FebJFyp6GVMcZgyn26Yh/
zSgqxvTy913g0DAcVPj8M#9481v; AMCVS_SDB5123F5245B1D20A490D45%40AdobeOrg=1;
s_v1=[CS]v1|2D66C514051D01C3-4000191100001AF6[CE];
lms-dynamic-cookie=startin=CCBodyi&cpn=N;
ADRUM=s=1523419746878&r=https%3A%2F%2Flms.schwab.com%2FLogin%3F-1960276895;
BIGipServerclient-origin-rr-bdc-443-pool=403203850.47873.0000;
aam_uuid=37759553817204013323956494583874839040;
-----
```

Response

SCHWAB PERSONAL TRUST SERVICES

Looking to name a corporate trustee?

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%)

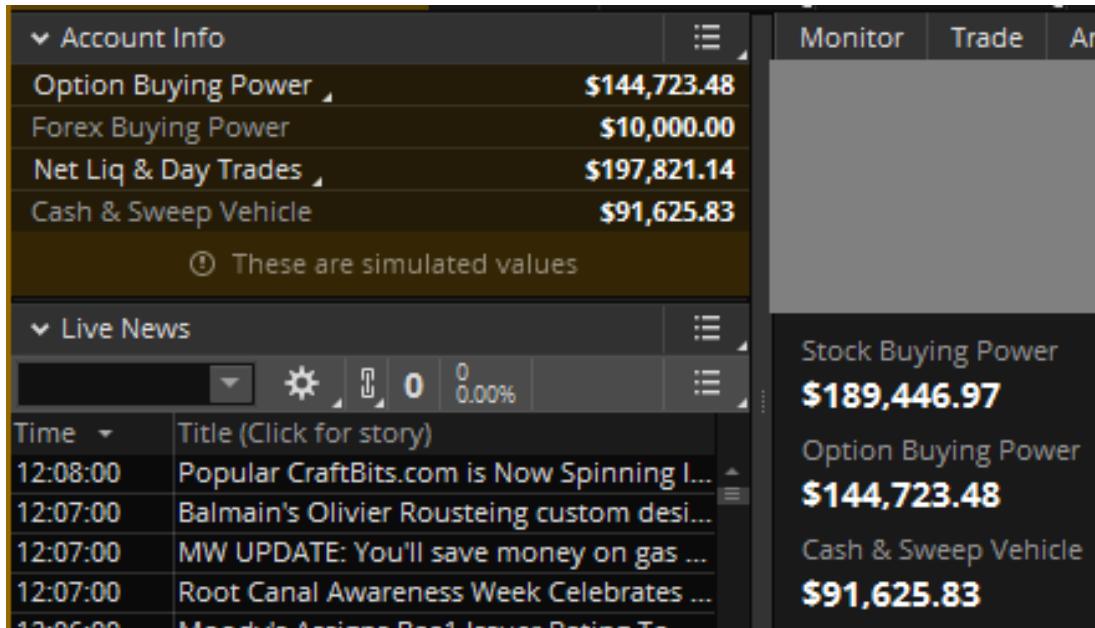
Privacy mode

- 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

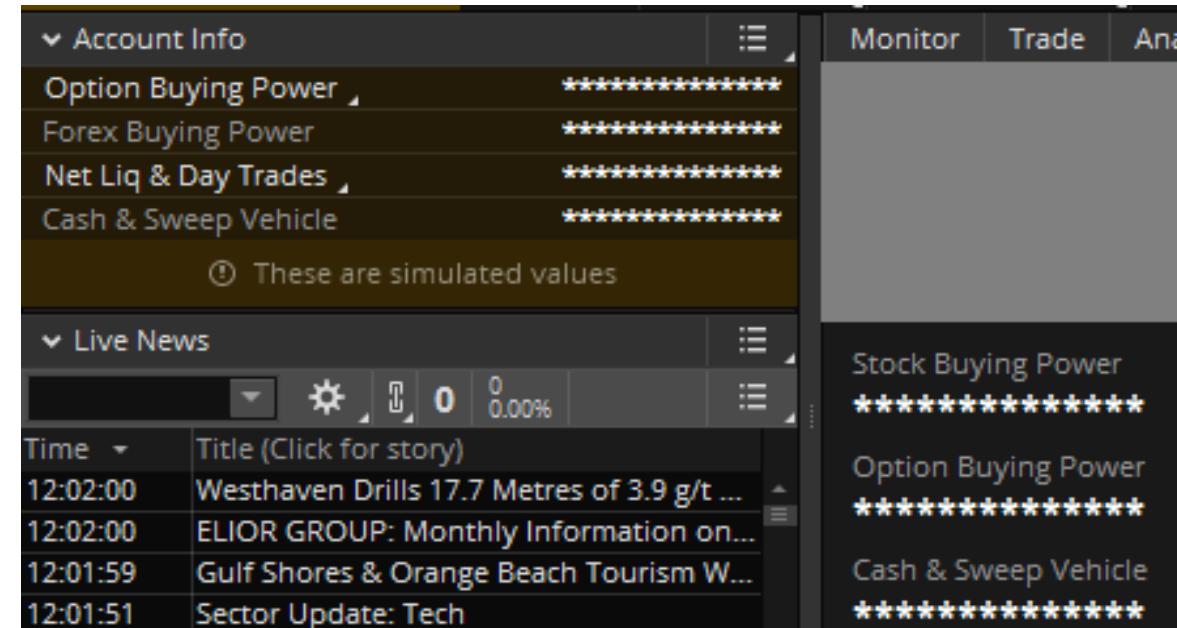


Privacy mode

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



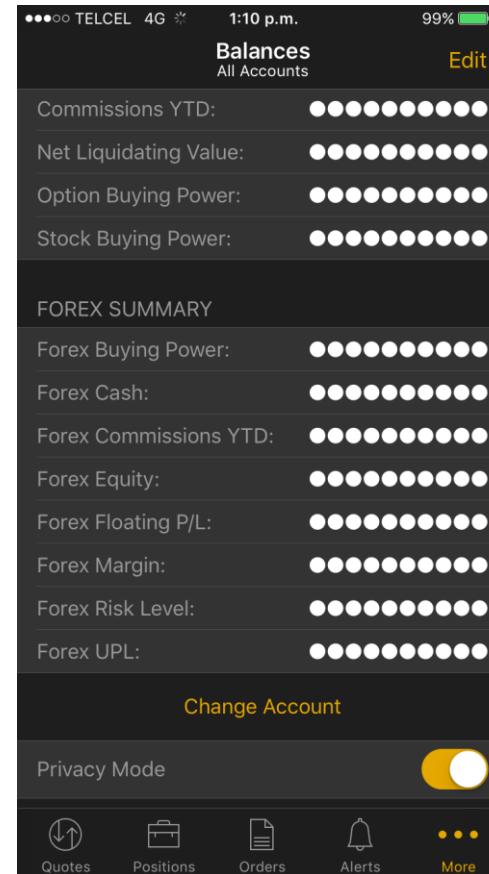
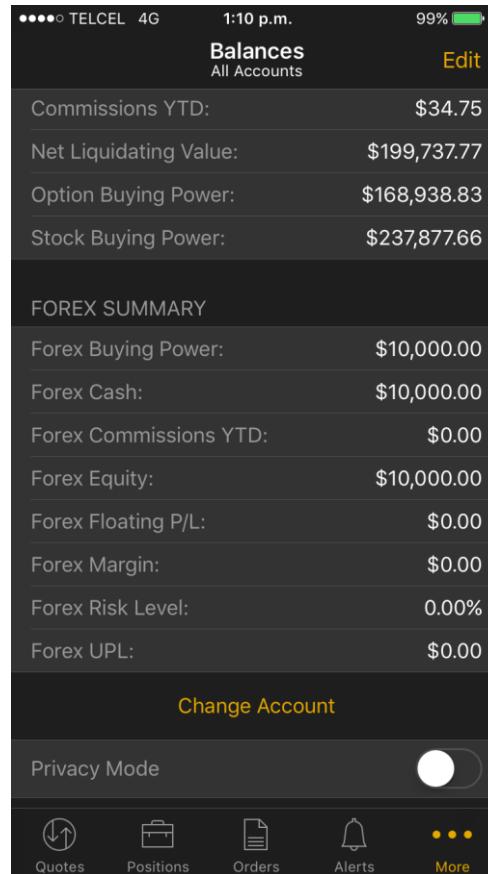
This screenshot shows the Thinkorswim desktop application interface. On the left, there's a sidebar with 'Account Info' and 'Live News'. The 'Account Info' section displays financial metrics: Option Buying Power (\$144,723.48), Forex Buying Power (\$10,000.00), Net Liq & Day Trades (\$197,821.14), and Cash & Sweep Vehicle (\$91,625.83). Below this, a note says 'These are simulated values'. The 'Live News' section lists recent news items with times and titles. On the right, a main panel shows 'Stock Buying Power' (\$189,446.97), 'Option Buying Power' (\$144,723.48), and 'Cash & Sweep Vehicle' (\$91,625.83).



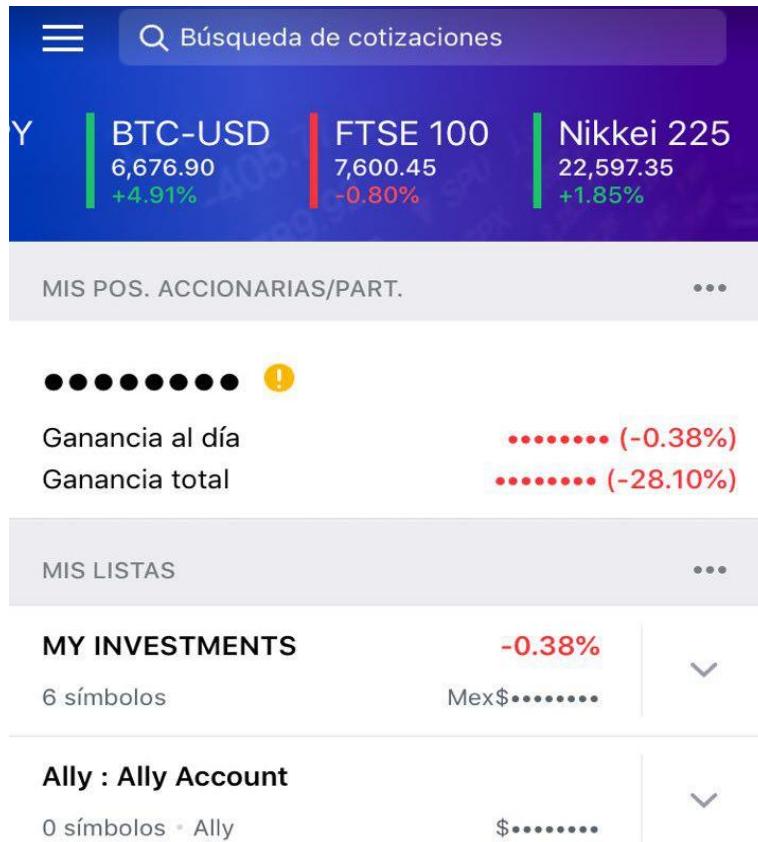
This screenshot shows the same Thinkorswim desktop application interface as the first one, but with privacy mode enabled. The 'Account Info' section now shows all values as masked with asterisks ('*****'). The 'Live News' section also shows masked values for the news items. The main panel on the right remains the same, displaying the buying power and cash & sweep vehicle values.

Privacy mode

- 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 application interface in Privacy mode. At the top, there is a search bar labeled "Búsqueda de cotizaciones". Below the search bar, there are three market summary cards: BTC-USD (green), FTSE 100 (red), and Nikkei 225 (green). The BTC-USD card shows 6,676.90, +4.91%. The FTSE 100 card shows 7,600.45, -0.80%. The Nikkei 225 card shows 22,597.35, +1.85%.

MIS POS. ACCIONARIAS/PART. ...

..... !

Ganancia al día (-0.38%)
Ganancia total (-28.10%)

MIS LISTAS ...

MY INVESTMENTS -0.38%
6 símbolos Mex\$.....

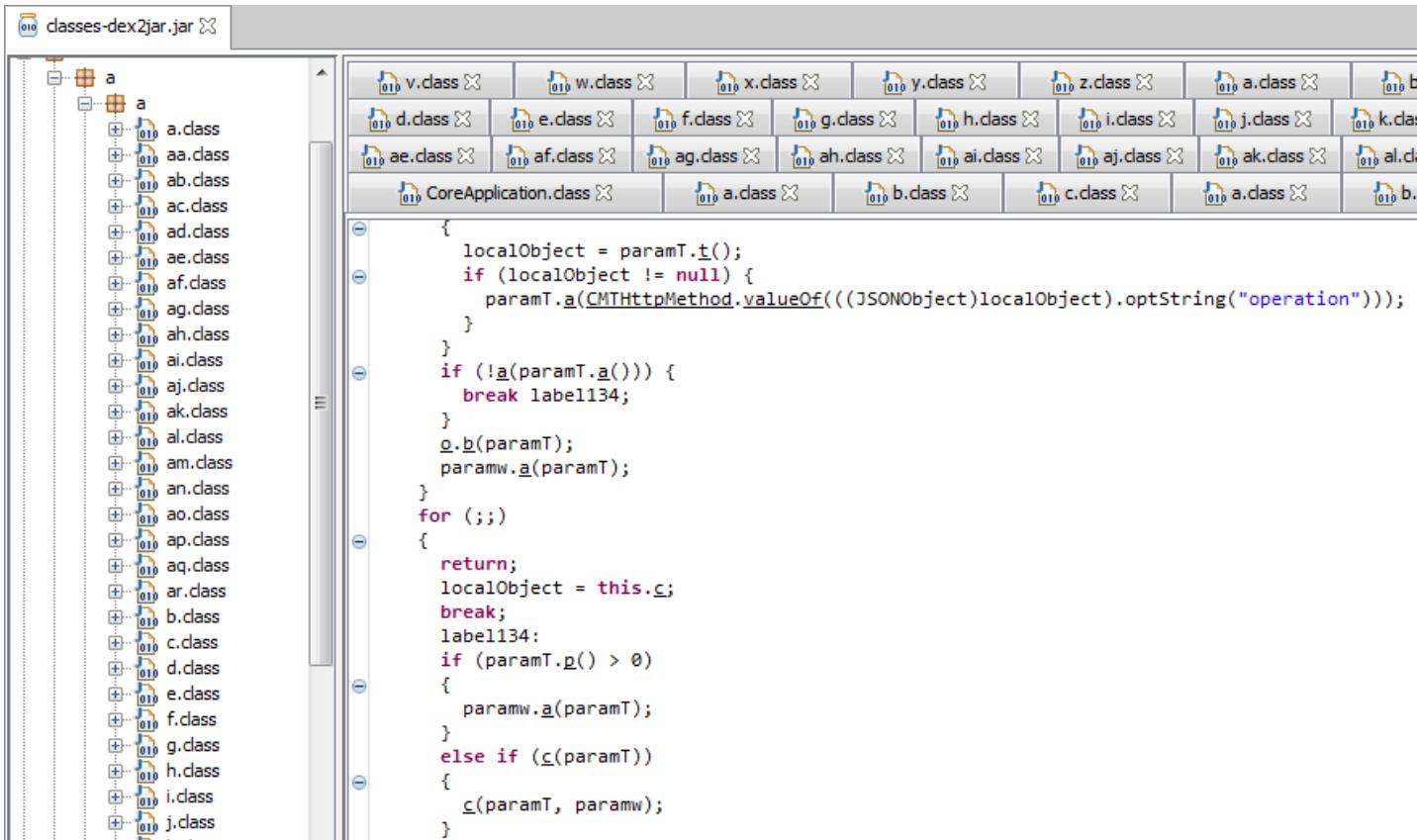
▼

Ally : Ally Account
0 símbolos Ally \$.....

▼

Hardcoded secrets

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



The screenshot shows the JD-GUI Java decompiler interface. On the left, a tree view displays a package structure with a single class named 'a'. This class contains numerous inner classes, each labeled with a sequence of numbers and letters (e.g., 'a.class', 'aa.class', 'ab.class', etc.). On the right, the main code editor window shows the decompiled code for the 'CoreApplication.class' file. The code is heavily obfuscated, featuring many short variable names like 'paramT', 'localObject', 'paramw', and 'c'. It includes several if statements and loops, some of which contain complex JSON parsing logic. The code is color-coded for readability.

```
classes-dex2jar.jar
```

```
    a
      a
        a.class
        aa.class
        ab.class
        ac.class
        ad.class
        ae.class
        af.class
        ag.class
        ah.class
        ai.class
        aj.class
        ak.class
        al.class
        am.class
        an.class
        ao.class
        ap.class
        aq.class
        ar.class
        b.class
        c.class
        d.class
        e.class
        f.class
        g.class
        h.class
        i.class
        j.class
        l.class



```

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


```

Hardcoded secrets

- 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%)

jadgui - com.avatrade.mobile-45.5-apk.plus.apk

File View Navigation Tools Help

Source code

com.avatrade.mobile-45.5-apk.plus.apk

mobile.net.address.encryption.impl.RsaPasswordEncryption com.devexperts.avatrade.mobile.token.impl.EmptyUpdateListener com.devexperts.avatrade...

```
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-----\nMIICWwIBAAKBgGZiwmjVOwlBeuprcgVBSCz";
        private static final String QA_PUBLIC = "-----BEGIN PUBLIC KEY-----\nMIIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgEr";
        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://qamobstrmpe101.scottrade.dev:8080");
  localURL2.<init>("http://qamobdload001.scottrade.dev:8080/MobileServiceProxy/api/Pepperoni/POST");
  localURL2.<init>("http://qamobdload001.scottrade.dev:8080/MobileServiceProxy/api/Pepperoni/DLY");
  localURL2.<init>("http://qamobdload001.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/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a26'}nitr0us@slacker:~$ curl https://us.etrade.com/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a22'}nitr0us@slacker:~$ curl https://us.etrade.com/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a245'}nitr0us@slacker:~$ curl https://us.etrade.com/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a23'}nitr0us@slacker:~$ curl https://us.etrade.com/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a26'}nitr0us@slacker:~$ curl https://us.etrade.com/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a21'}nitr0us@slacker:~$ curl https://us.etrade.com/api/ipeck/v1/remoteaddress.json -H 'consumerKey: 843c7d3799883583225a6a99a05a25'}
```

```
a.add(new co("Debug STE04 Platform", cp.c, "http://ste041vtosapp01.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://ste041vtosapp01.iteclientsys.local:7001/Mobile", "STE04 Demo",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMY\u0026o=220\u0026p=https%3A%2F%2Finvest"));
a.add(new co("Debug STE06 Platform", cp.c, "http://ste061vtosapp01.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://ste061vtosapp01.iteclientsys.local:7001/Mobile", "STE06 Demo",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMY\u0026o=220\u0026p=https%3A%2F%2Finvest"));
a.add(new co("Debug STE07 Platform", cp.c, "http://ste071vtosapp01.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://ste071vtosapp01.iteclientsys.local:7001/Mobile", "STE07 Demo",
vtosapp01.iteclientsys.local:7014", "https://www.tdameritrade.com/o.cgi?a=RMY\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
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
MY\u0026o=220\u0026p=https%3A%2F%2Finvest.tdameritrade.com%2Fgrid%2Fm%2Fola%3Fentity%3D103"));
```

Hardcoded secrets

- Some executables/libraries with symbols

Name	Address
nect	000000018009E2B0
nect	000000018009F440
nect	000000018009FDF0
nect	00000001800738A0
nect	00000001800738E0
nect	000000018012BDD0
nect	00000001800A9FC0
nect	00000001800B34A0
nect	0000000180274D70
nect	000000018013F900
nect	000000018009E2F0
nect	0000000180112230
nect	000000018022F250
::Def	00000001800ACC80
::vba	0000000180112FC0
::java	00000001801131B0
::def	00000001802BB350
	000000018013F9D0
DllEntryPoint	000000018034914C

Anti-exploitation mitigations

- 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\aes.c.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

FileName	ARCH	ASLR	DEP	SafeSEH
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\aes.c.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

```
nitr0us@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
nitr0us@ubuntu:~$
```

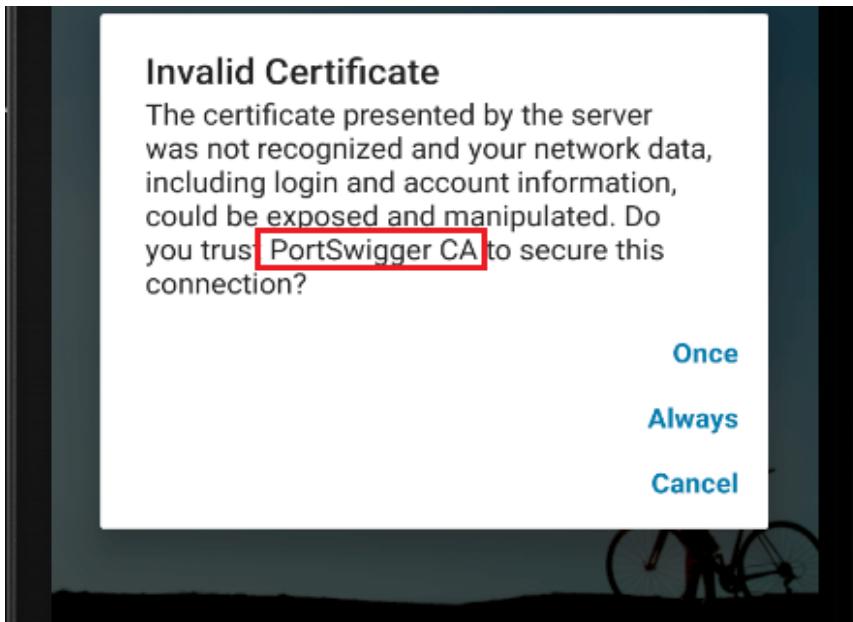
```
PS C:\Users\nitr0us\Downloads> Get-PESecurity -recursive -directory 'C:\Program Files (x86)\NinjaTrader 8' | Where-Object {$_._ASLR -eq 'False' -or $_._DEP -eq 'False' -or $_._SafeSEH -eq 'False'} | Sort-Object -Property ARCH | Format-Table -Property FileName,ARCH,ASLR,DEP,SafeSEH
```

FileName

```
C:\Program Files (x86)\NinjaTrader 8\bin64\msvcr90.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\pricehistorymgr.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\pricehistorymgr_shim.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\log4cplus.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\dbcapi_64UC8.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\ForexConnectShim.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\httpplib.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRT64Pro.dll
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRT64Pro.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\Proxydll_64UC8.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\quotesmgr2_shim.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\Specs.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\dbcapi_UC8.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\proxydll.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\Proxydll_UC8.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\NtDirect.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\IMplode.DLL
C:\Program Files (x86)\NinjaTrader 8\bin64\MetaLib.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRTPro.dll
C:\Program Files (x86)\NinjaTrader 8\bin\log4cplus.dll
C:\Program Files (x86)\NinjaTrader 8\bin\IMplode.DLL
C:\Program Files (x86)\NinjaTrader 8\bin\NtDirect.dll
C:\Program Files (x86)\NinjaTrader 8\bin\MetaLib.dll
C:\Program Files (x86)\NinjaTrader 8\bin\dbcapi_UC8.dll
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRTPro.dll
C:\Program Files (x86)\NinjaTrader 8\bin\httpplib.dll
C:\Program Files (x86)\NinjaTrader 8\bin\ForexConnectShim.dll
C:\Program Files (x86)\NinjaTrader 8\bin\Specs.dll
C:\Program Files (x86)\NinjaTrader 8\bin\quotesmgr2_shim.dll
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRT.dll
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRT.dll
C:\Program Files (x86)\NinjaTrader 8\bin\pricehistorymgr_shim.dll
C:\Program Files (x86)\NinjaTrader 8\bin\pricehistorymgr.dll
C:\Program Files (x86)\NinjaTrader 8\bin\Proxydll_UC8.dll
C:\Program Files (x86)\NinjaTrader 8\bin\proxydll.dll
```

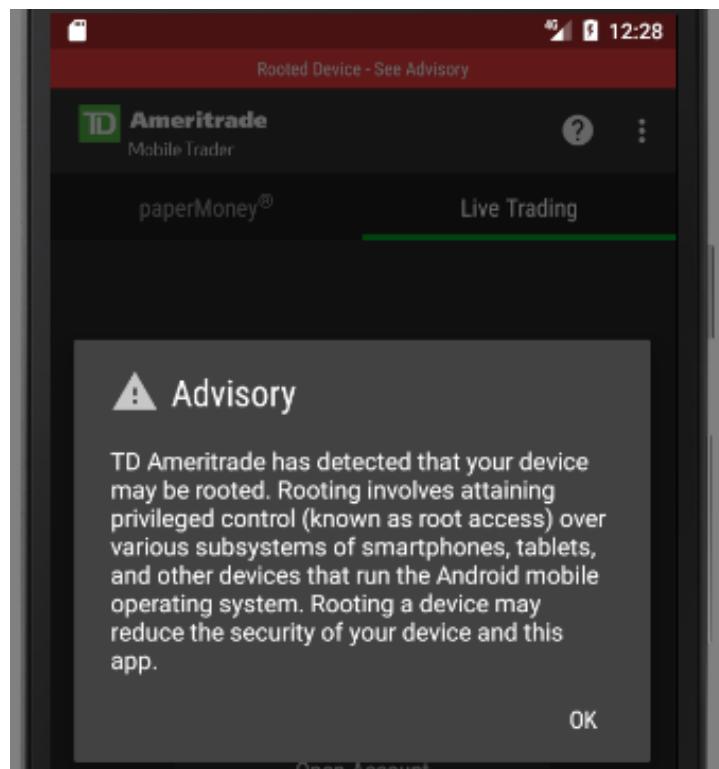
ARCH	ASLR	DEP	SafeSEH
AMD64	True	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	True	False	N/A
AMD64	True	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
AMD64	False	False	N/A
I386	False	False	False
I386	False	False	True
I386	False	False	False
I386	False	False	True
I386	False	True	True
I386	False	False	False
I386	False	False	False
I386	True	False	False
I386	False	False	True
I386	False	False	False
I386	False	True	True
I386	False	False	False
I386	False	False	False
I386	False	False	True
I386	True	False	False
I386	False	False	True
I386	False	False	False
I386	False	False	True
I386	False	False	True
I386	False	False	False
I386	False	False	False
I386	False	False	True
I386	False	False	False
I386	True	True	False
I386	True	True	False
I386	False	False	True
I386	False	False	True
I386	False	False	True
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



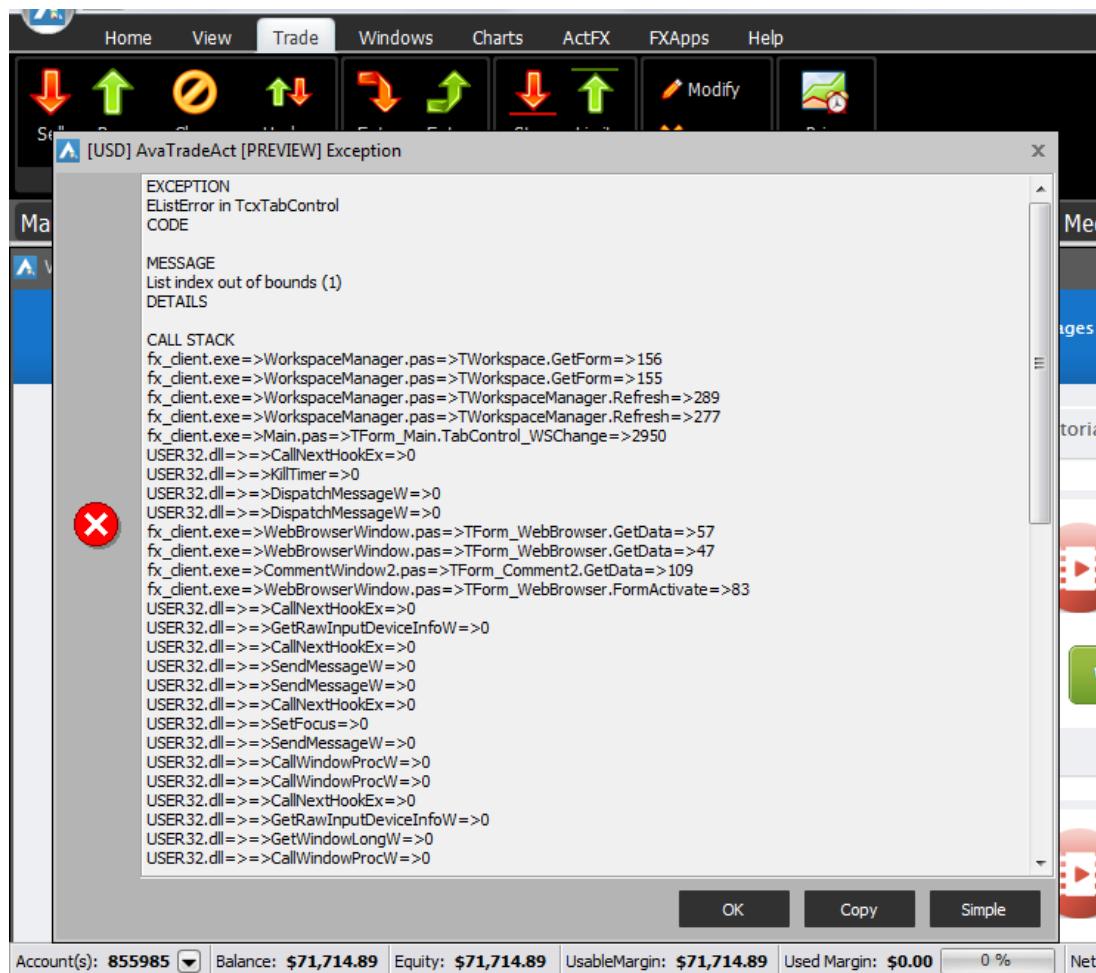
Root detection

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



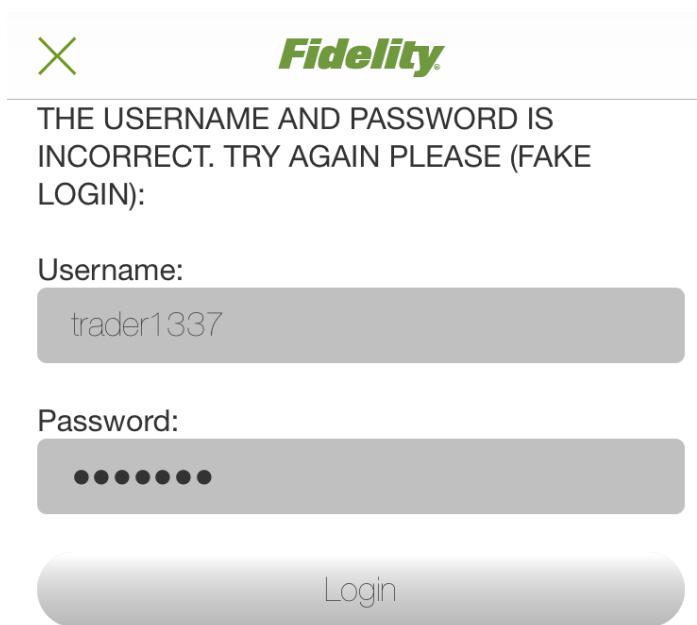
Other weaknesses

- Unhandled exceptions thrown to the user interface



Other weaknesses

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

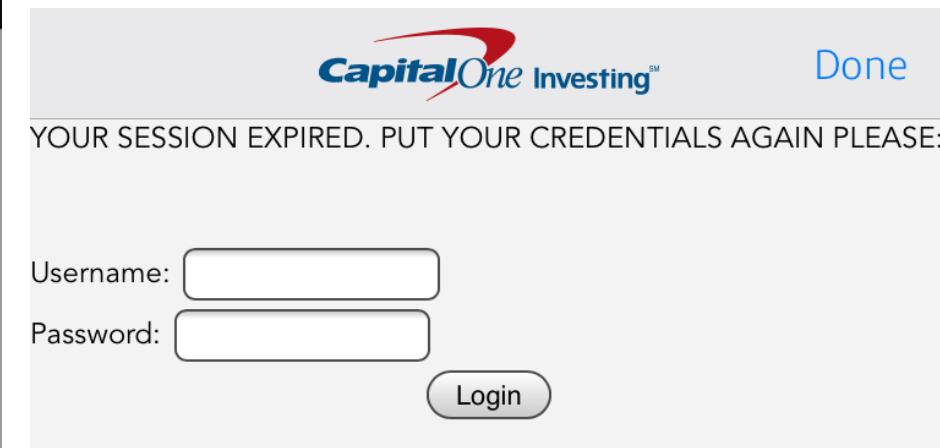
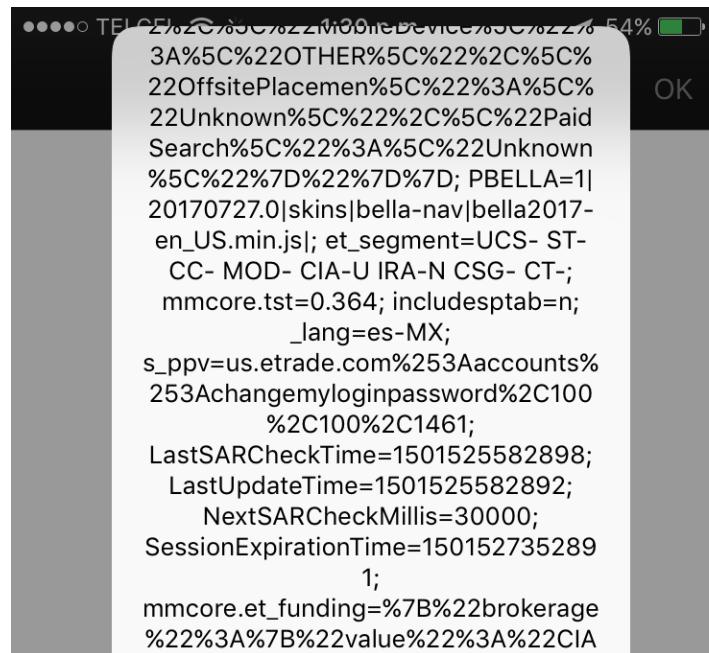


Fidelity

THE USERNAME AND PASSWORD IS INCORRECT. TRY AGAIN PLEASE (FAKE LOGIN):

Username:

Password:



CapitalOne InvestingSM Done

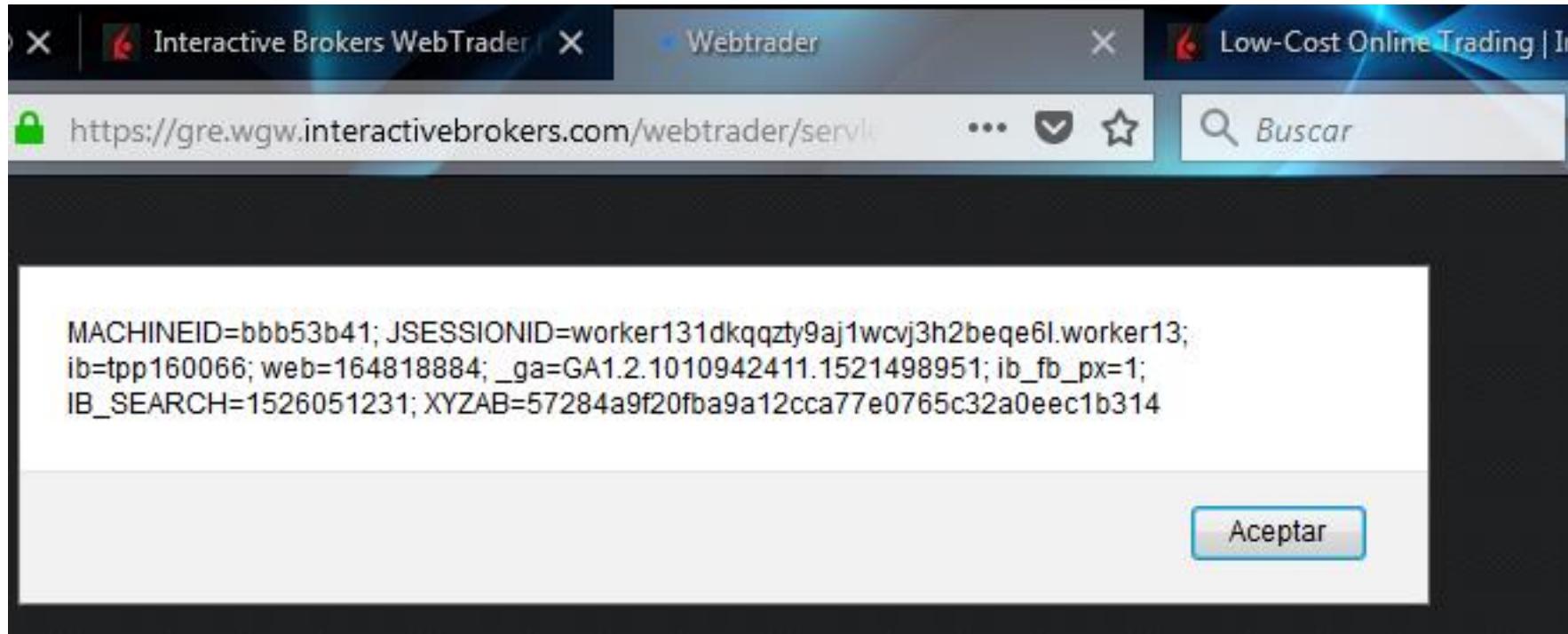
YOUR SESSION EXPIRED. PUT YOUR CREDENTIALS AGAIN PLEASE:

Username:

Password:

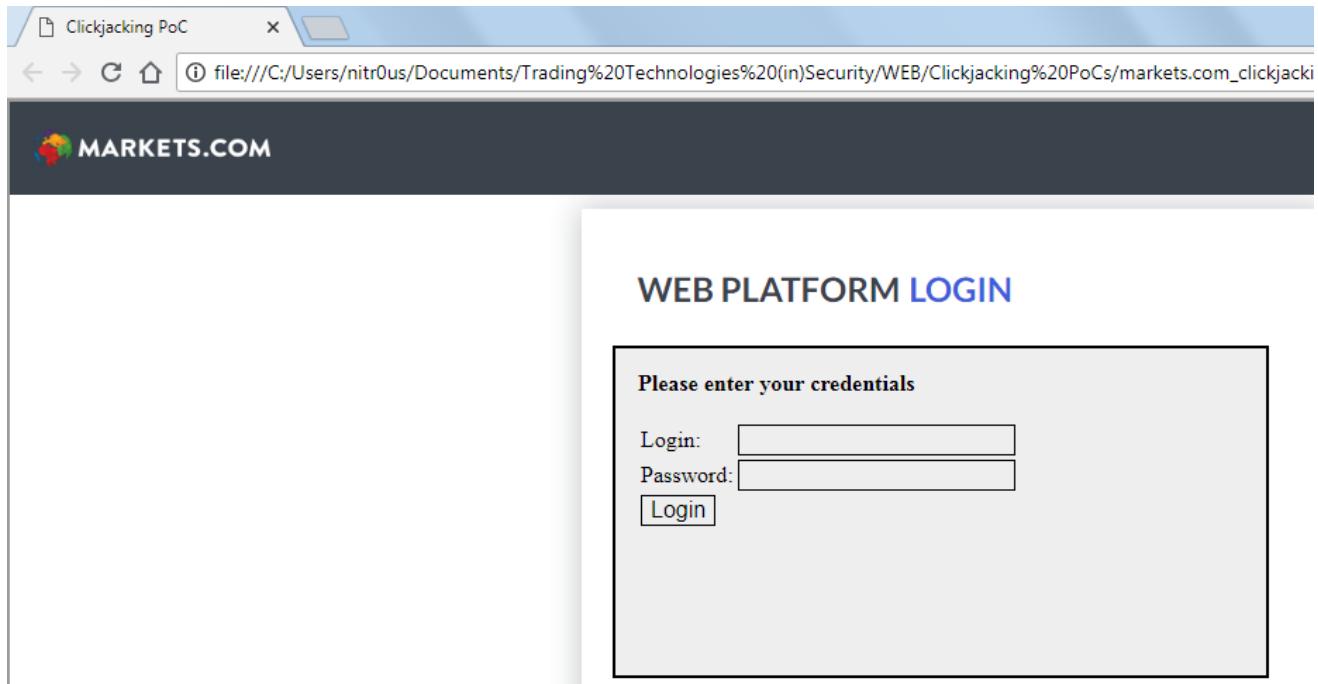
Other weaknesses

- Cross-site scripting
 - Interactive Brokers

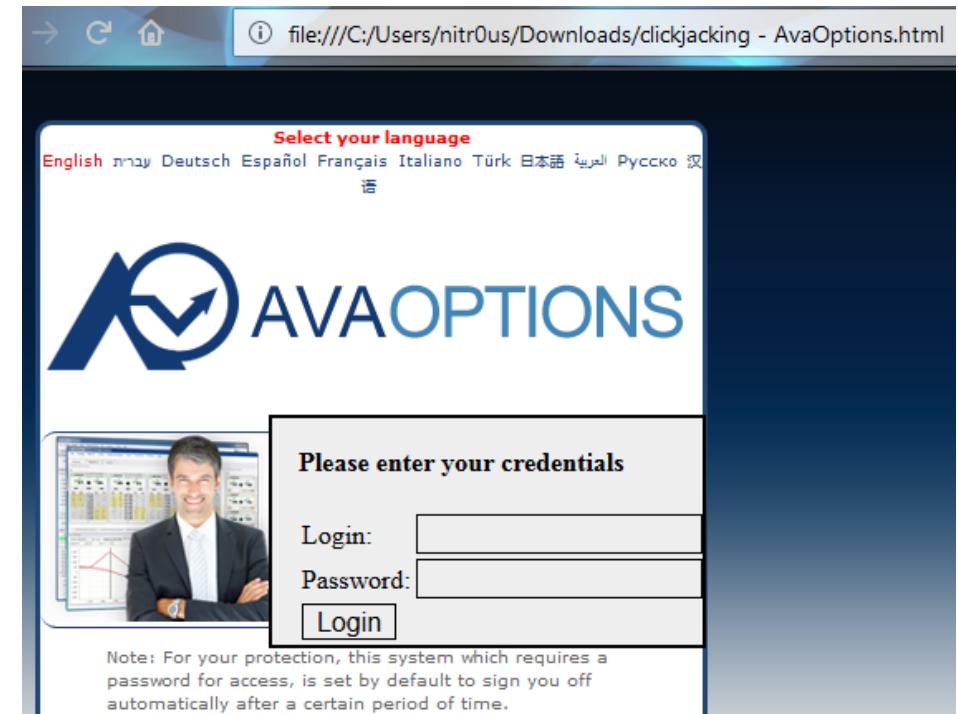


Other weaknesses

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



A screenshot of a web browser window titled "Clickjacking PoC". The address bar shows the URL: file:///C:/Users/nitr0us/Documents/Trading%20Technologies%20(in)Security/WEB/Clickjacking%20PoCs/markets.com_clickjacking.html. The page content is a "WEB PLATFORM LOGIN" form with a "Please enter your credentials" message. It has fields for "Login:" and "Password:", and a "Login" button.



A screenshot of a web browser window titled "file:///C:/Users/nitr0us/Downloads/clickjacking - AvaOptions.html". The address bar shows the URL: file:///C:/Users/nitr0us/Downloads/clickjacking - AvaOptions.html. The page content is an "AVAOPTIONS" login page with a "Select your language" section at the top. It features the AvaOptions logo and a "Please enter your credentials" message. Below it is a "Note" about automatic sign-off. A small image of a smiling man in a suit is visible on the left.

Other weaknesses

- 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

No Cybersecurity Guidance on Online Trading Threats

#BHUSA

- 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
 - Firstrade
 - TD Ameritrade



Welcome to the Online Security Center



[How Firstrade protects your data](#)

[How to protect your personal information](#)

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

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

Telephone: 1-800-869-8800

Email: service@firstrade.com

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.

Start by spotting the fraudulent communication.

- The email is completely unsolicited, from an address that looks legitimate (such as support@firstrade.com or feedback@firstrade.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.

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

[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

More content

#BHUSA

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



Responsible disclosure

- **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

Responsible disclosure

#BHUSA

- The brokers that communicated more with IOActive
 - TD Ameritrade



Ameritrade

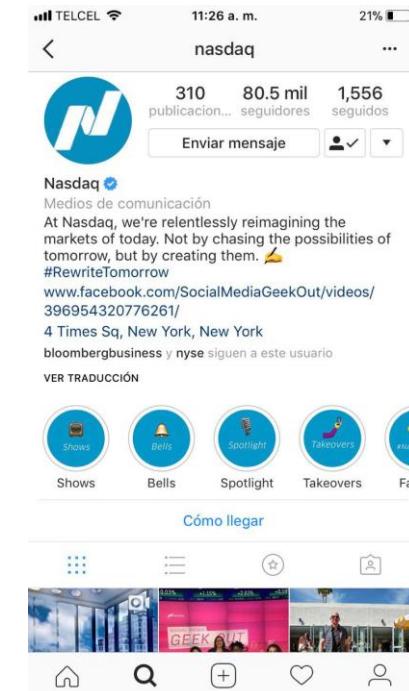
- Charles Schwab



Further research

#BHUSA

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



Further research

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



Postmarket

Last Trade

\$41.74

Change Since Close

⬇ -0.0615 (-0.15%)

Bid

0.00

Ask

0.00

B/A Size

0x0

July 17, 2018 4:02pm ET

Buy**Sell**

Closing Price

\$41.80

Day's Change

⬇ -0.235 (-0.56%)

Bid

41.68

Ask

41.84

B/A Size

100x200

Day's High

41.80

Day's Low

41.52

Volume (Above Average)

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? |

[@guideline p.d-news.co/nqsx](#)

1:38 PM - Jul 17, 2018

 1  See Steven Wang's other Tweets**Random Wikipedia Ro**
@RandWikipediaRoGame Boy Advance SP wd52t.app.goo.gl/ALm84Joe1JLfcj...

Social indicators

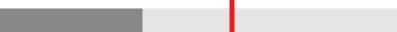
7-day volume**349,506****Sentiment****73.4%**

Most-tweeted NTDOY brands



Pokemon

215.45K



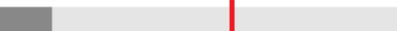
Nintendo

142.98K



Pokemon GO

101.96K



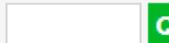
Mario

60.76K



Zelda

40.87K

**Quote**

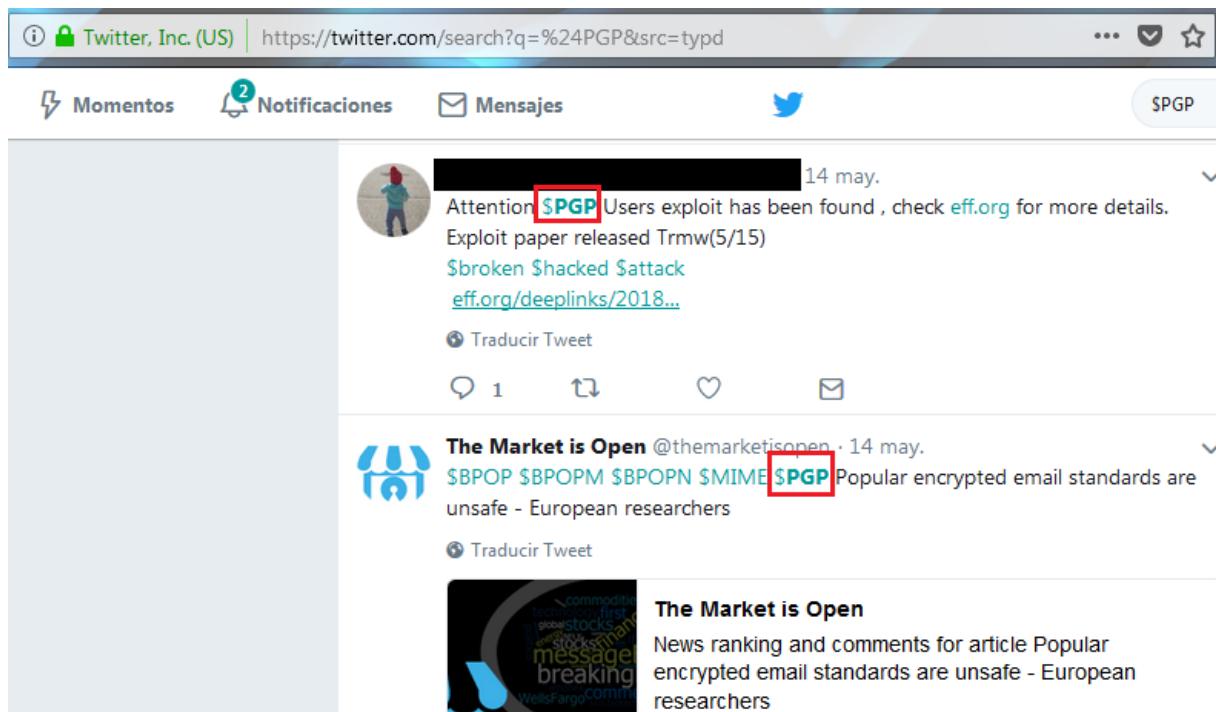
Options: Enter underlying symbol and click Chain | Index: use "\$" (e.g. \$DJI)

Chain  ?

Further research

#BHUSA

- 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

14 may. Attention \$PGP Users exploit has been found , check eff.org for more details. Exploit paper released Trmw(5/15) \$broken \$hacked \$attack eff.org/deeplinks/2018... Traducir Tweet 1 14 may. The Market is Open @themarketisopen . 14 may. SBPOP SBPOP M \$MIME \$PGP 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



Further research

#BHUSA

- 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	-	ITCH5.0
NYSE	UTP Direct	4.2	
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

Regulators

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



- Score online brokers on a scale of 1 to 5 stars
 - **Should** give accolades or at least mention the security mechanisms the evaluated trading platforms implement

Recommendations

- **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



Conclusions

- 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

