


# Threats in a virtual world

Charlie Eriksen

Security Analyst

CCP


PUFFINS
GONNA
PUFF

# Agenda

- EVE 101
- Threat landscape
- Goals
- The arms race thus far
- Next steps and conclusion

# Prior work


DEFCON 19: Hacking MMORPGs for Fun and Mostly Profit

# Prior work

metr0


Defcon 18 - Securing MMOs: A Security Professional's View From the Inside

# Prior work


Exploiting Online Games: Virtual World Security-Greg Hoglund


EVE
ONLINE
COPYRIGHT © CCP GAMES 1997 - 2009

# EVE 101

- Single-sharded universe
  - Cluster specifically for China
- Over half a million players
- All players can interact with each other
- More than 2000 players can be in the same solar system at the same time
- You mine, manufacture, trade, and kill each other
- The economy is extremely similar to the real world economy
- All actions have impact and everybody can make a difference
- Losses have consequences, so you need money to do more fun things

# TRANQUILITY DOWNTIME ON SUNDAY, JUNE 2 AND MONDAY, JUNE 3

03.06.2013 03:41 | By CCP Spielmann

At 02:05 UTC June 2nd, CCP became aware of a significant and sustained distributed denial-of-service attack (DDoS) against the Tranquility cluster (which houses EVE Online and DUST 514) and web servers.

Our policy in such cases is to mobilize a taskforce of internal and external experts to evaluate the situation. At 03:07 UTC, that group concluded that our best course of action was to go completely offline while we put in place mitigation plans.

While we initially reopened EVE Online and DUST 514, at 14:51 UTC we became aware of additional information that led us to re-evaluate our decision. With the highest sense of precaution we took the decision to take Tranquility and associated websites back down for further investigation and an exhaustive scan of our entire infrastructure.

What we can now confirm is that a person was able to utilize a vulnerability in one of the back-end services that support the operation of the Tranquility server. This vulnerability has now been secured and thoroughly tested.

We would like to stress that at no time was customer data compromised or accessible in any way.

The effort of returning the complex server structure of the EVE Universe and associated websites to service in a methodical and highly-scrutinized fashion began hours ago and Tranquility has now been brought online (at 10:13 UTC). Our teams will monitor the situation carefully in the coming hours to ensure that our services are accessible and that all customer data remains secure.

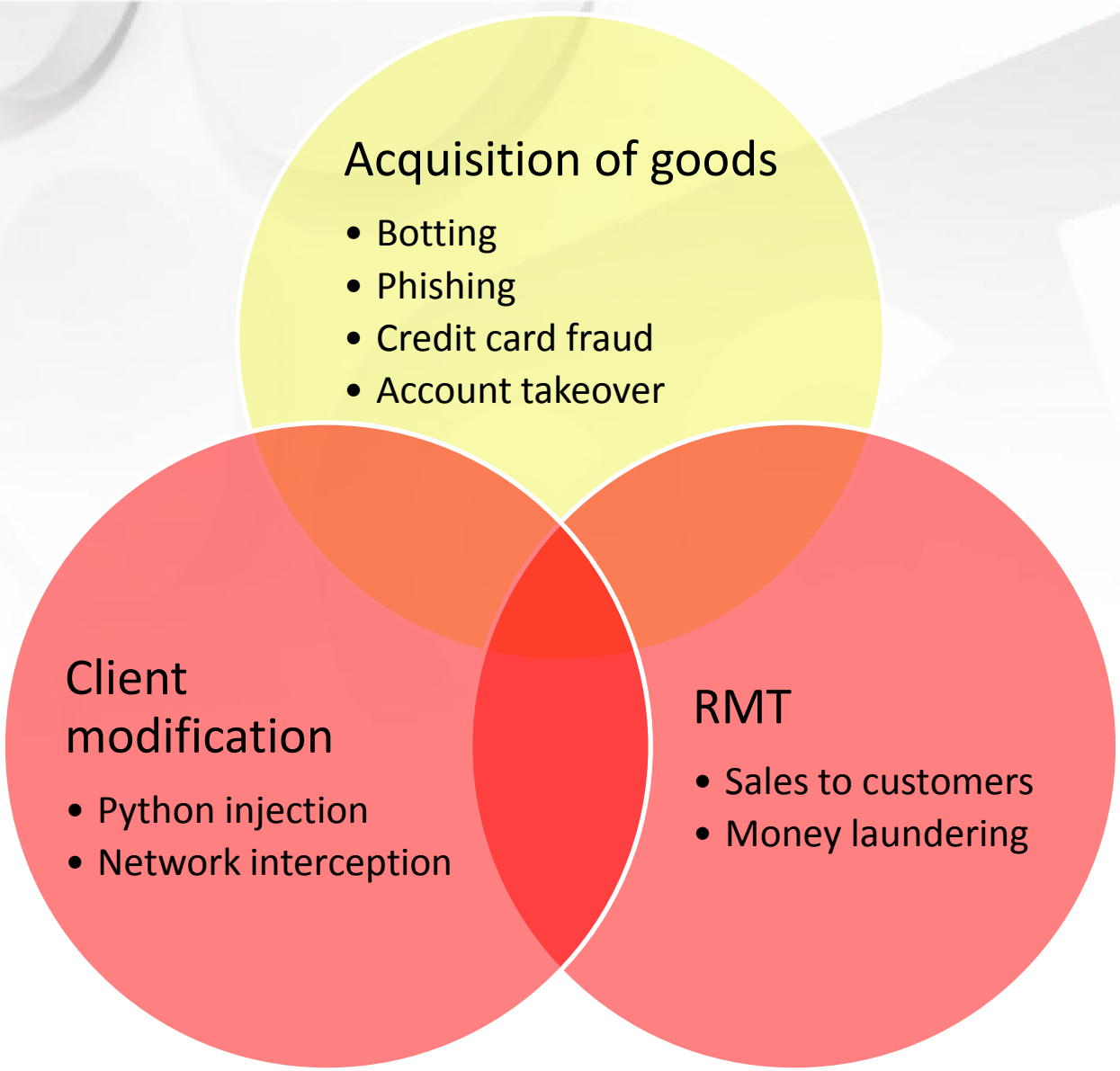
We will be looking at ways to compensate players in both EVE and DUST for the outage and expect to announce what that compensation will be very soon.

We would also like to take this opportunity to thank all of our players on EVE Online and DUST 514 for their patience and understanding during this unexpected downtime and the investigation. We are grateful for your support, as always.

Regards,
Jón Hörðdal Jónasson,
Chief Operating Officer
CCP


# How to tackle the issue?

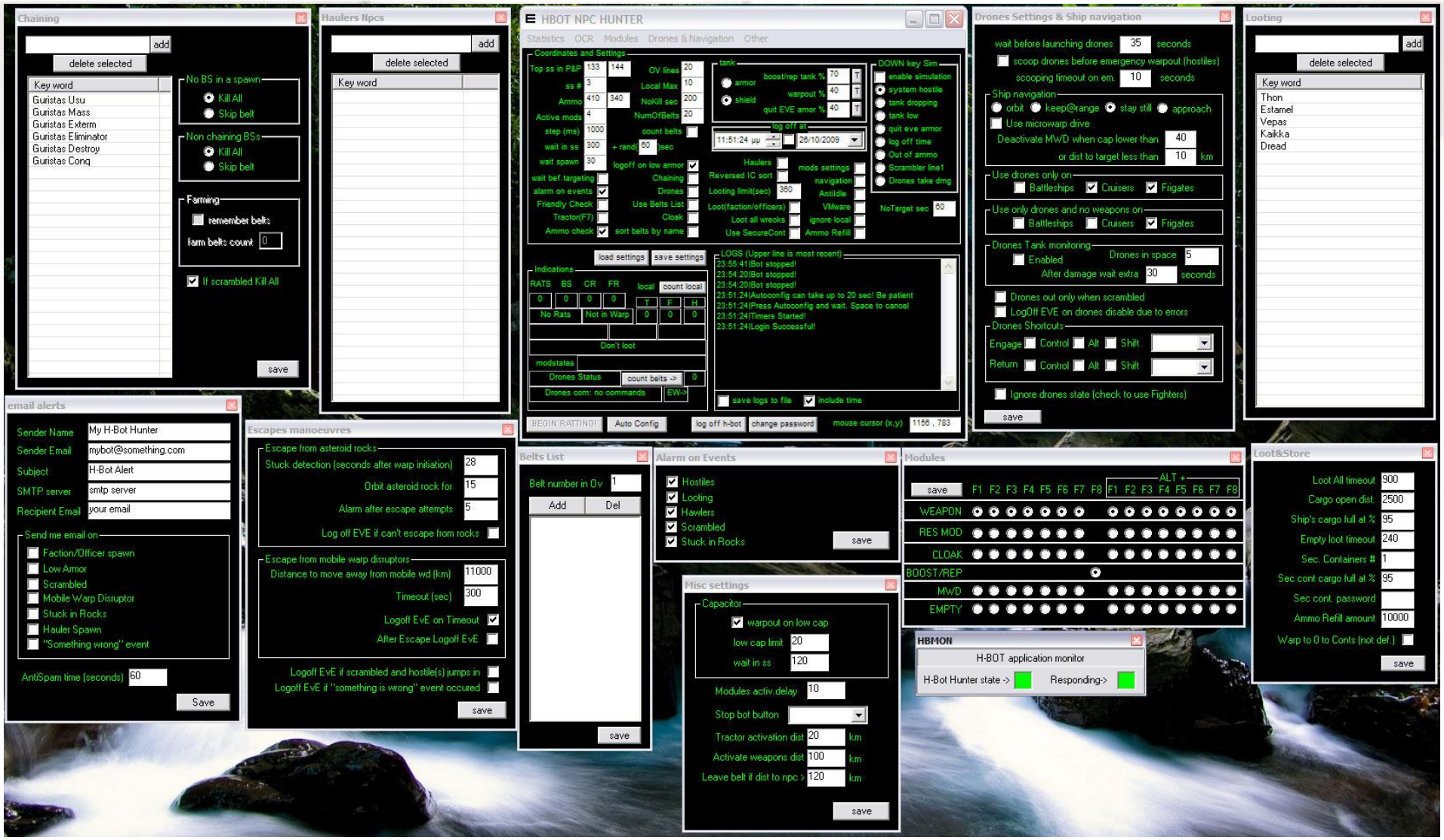
# Threat landscape



# Botting 101

- Acquiring wealth in EVE takes time
- Wealth in EVE is power
  - 1. Automate wealth acquisition
  - 2. Create a “bot farm” using said automation
  - 3. Sell the wealth for $$$
  - 4. ????
  - 5. PROFIT!!!!!

# Screen scraping bots



# Account hacking

- Common approaches:
  - Compromising third party sites
  - Account details on RMT sites
  - Phishing
- Accounts are liquidated and currency laundered to sales accounts(More later)

# Credit card fraud

- Classic money laundering
  1. Steal credit cards($$$)
     - At times this stems from real money trading companies
  2. Buy in-game currency through CCP(Virtual items)
  3. Sell the virtual items for ($$$$)
  4. ???
  5. PROFIT
- Of course, we get charge backs on the money

# Credit card fraud

*“…..the kinds of fraud that concern us the most, are the actual credit card frauds….*

*….I would dare anybody to ask an exec at a gaming company how much they've had to pay in Master Card and Visa fines, because of fraud”*

- Scott Hartsman, former Chief Creative Officer

and Executive Producer, RIFT, July 2011

Source: Nosy Gamer Blog - http://bit.ly/14VOWcY

# Credit card fraud

*“A lot of these farmers are essentially stealing from us. …. They use the account for a month, and then they call the credit card company and charge it back. We have suffered nearly a million dollars just in fines over the past six months; it's getting extremely expensive for us”*

- John Smedley, CEO, Sony Online Entertainment, January 2008

Source: Nosy Gamer Blog - http://bit.ly/14VOWcY

# Credit card fraud

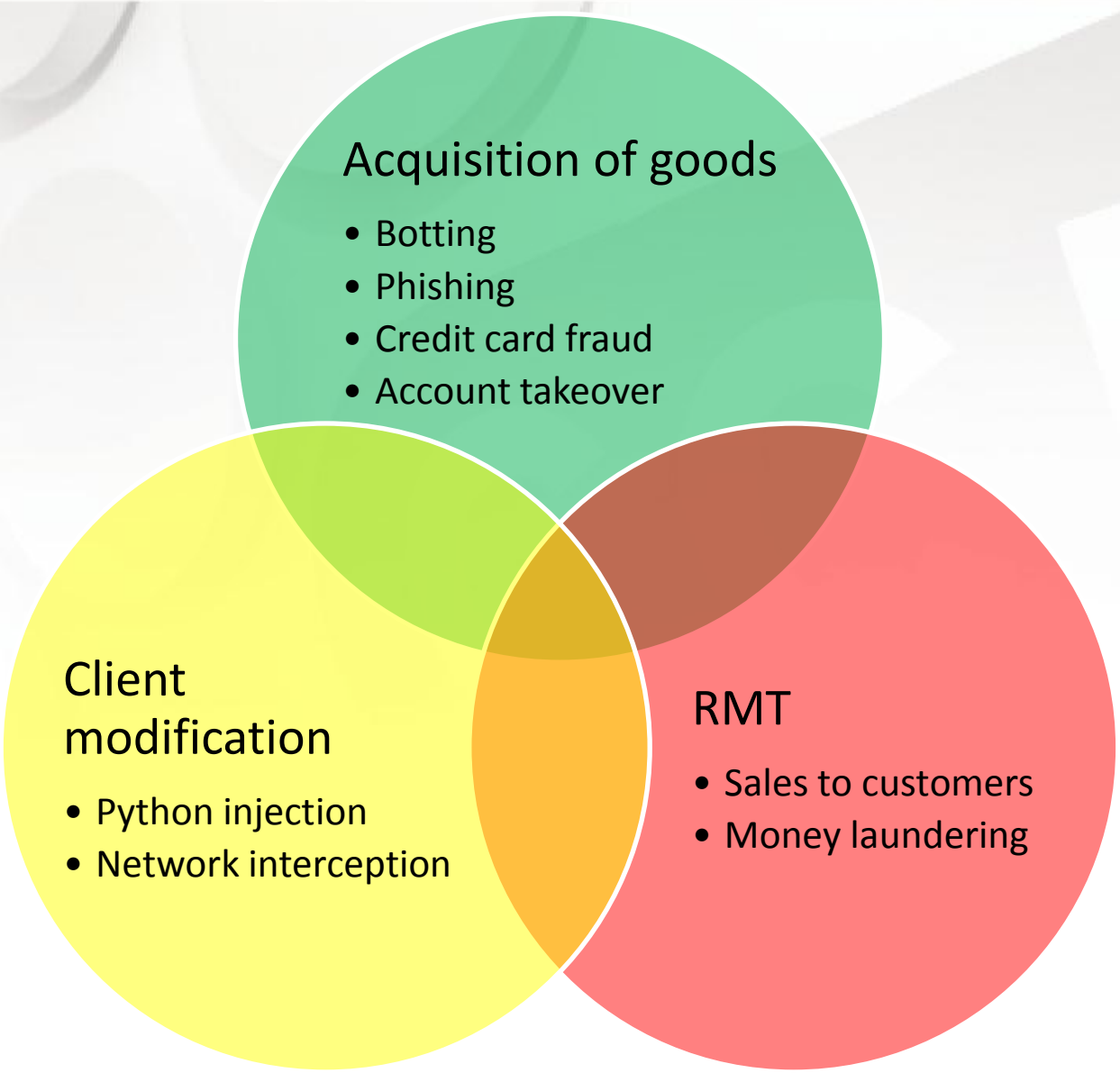
*"The problem comes in when they start doing other illegal activities. One of the biggest is the use of stolen credit cards….*

*It brings a terrible financial burden to us, not to mention the other problems we might have legally or financially around this."*

-Imre Jele, former head of game content (Producer), Jagex, February 2008

Source: Nosy Gamer Blog - http://bit.ly/14VOWcY

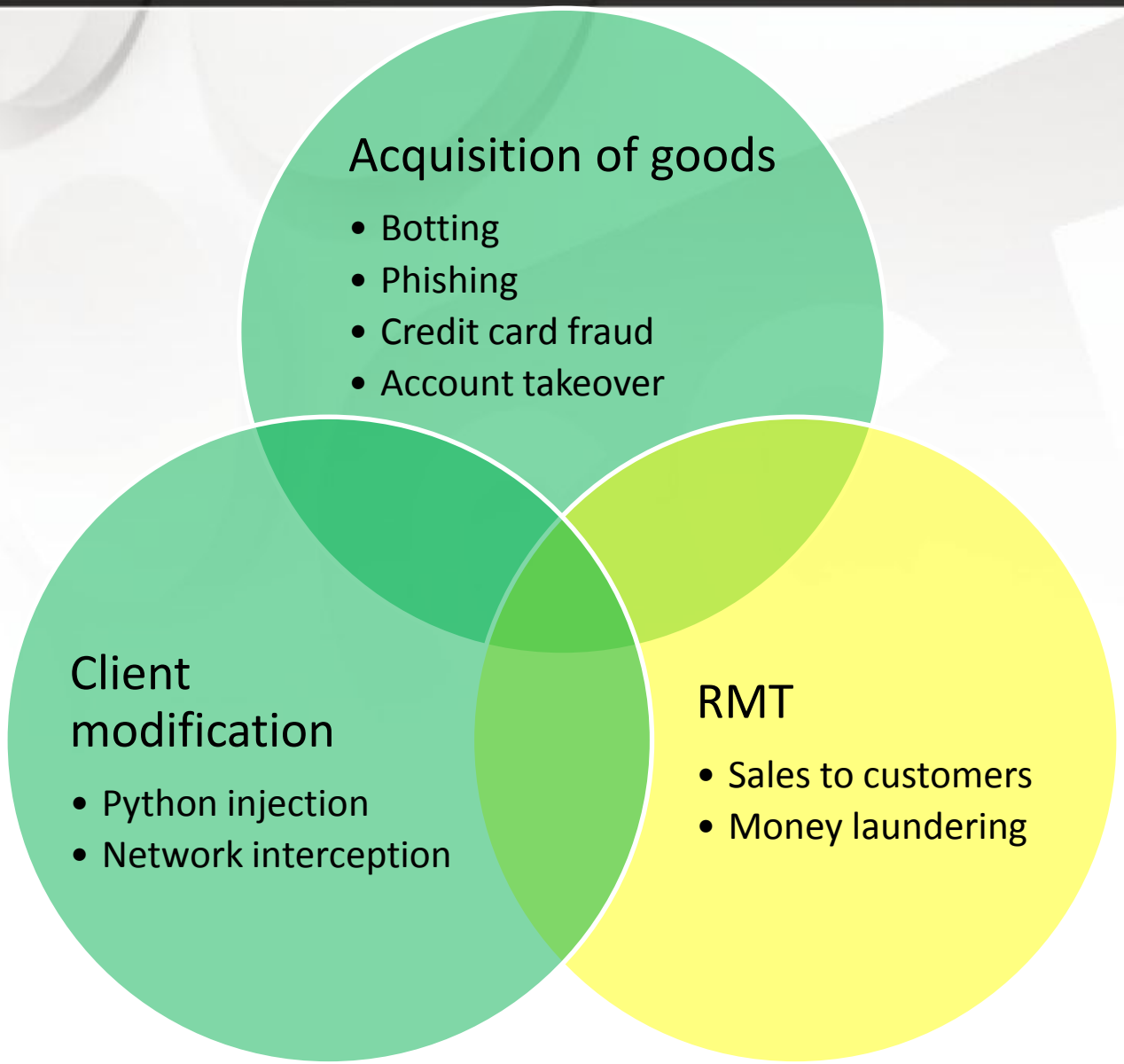
# Threat landscape



# Client modification

- Code injection
  - Making the client dance!
  - Trivial due to our use of python
    - Slightly customized Stackless Python
  - Very powerful in that it gives you full API access
- Network injection
  - Only recently started popping up
  - Gives you a lot of the same capabilities as code injection
  - Makes the client proxy through a middle-man and resigns the encryption on the socket

# Threat landscape



# Real money trading

- Turns virtual currency and items into $$$
- If there's a demand for in-game currency for $$$ from players, there's a supply.

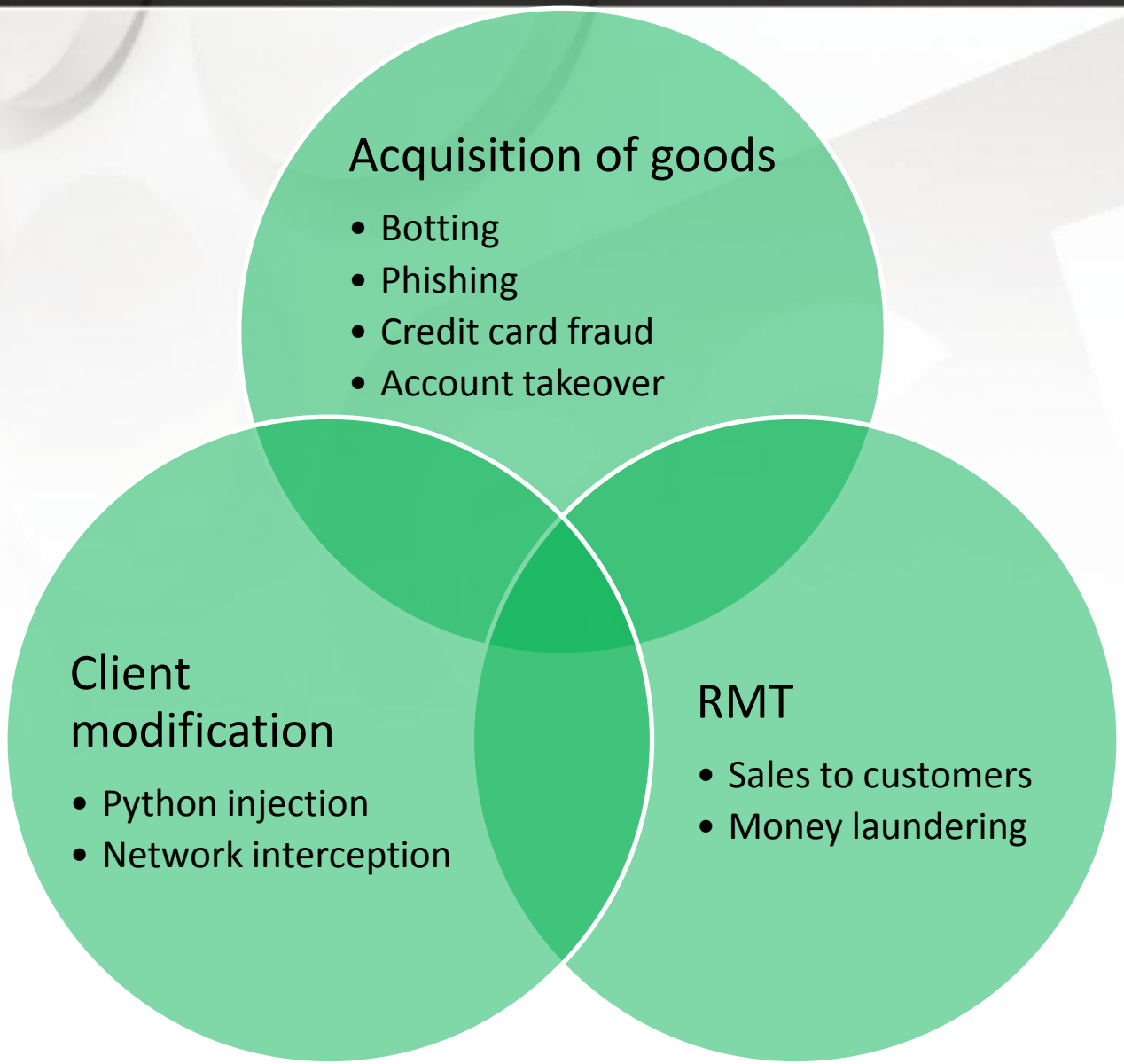
# Money laundering

- Money needs to be white-washed to decrease risk of detection
- Transferring value between currencies and items
- Transferring value between characters
- Plausible deniability for the bad guys
- Creates a lot of signal, which makes it easier for us

# Sale of in-game currency to customers

- Often also done through laundering “techniques”
  - Done to decrease risk of the operation
- Sticks out like a sore thumb, thankfully!
- Plausible deniability becomes a problem

# Threat landscape



# Reality check

1. You can not estimate the scope of the problem
2. If there's a demand, there's a supply
3. You do not have infinite resources
4. At some point the ROI is going to be =< 0

# Goals

- Create long-term goals and solutions
- “Solve” one piece of the puzzle at a time
  - RMT
  - Botting
  - Client modification
  - Account hacking

# 30 Day Pilot License Extension(PLEX)

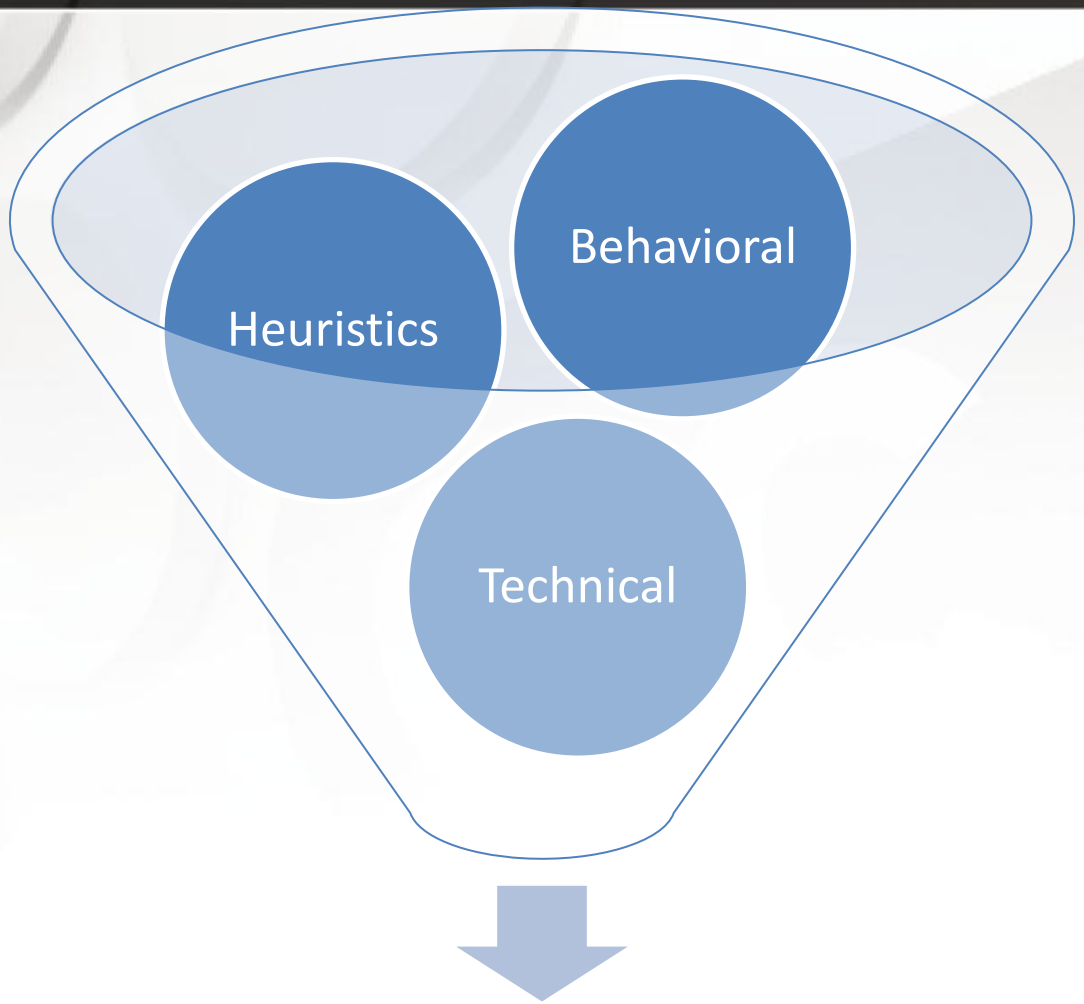
- An in-game item
- Can be bought for 15 euros/20 USD
- Consuming it will extend your subscription by 30 days
- Can be sold on the player-driven market for in-game currency
- Provides legal outlet for buying in-game currency for real currency
- RMT competes with the PLEX

# STEP 1- INCREASE BARRIER TO ENTRY ON BOTTING

# Goals

- Drive up cost of doing business
  - Decrease profitability per account
  - Increase amount of accounts needed
  - Increase hardware and infrastructure cost
- Hammer down on botting accounts
  - Prevent people botting 24/7
- Slowly increase the pressure
- Decrease the profitability of each bot account
- Drive the behavior under ground

# Data crunching




Risk profile

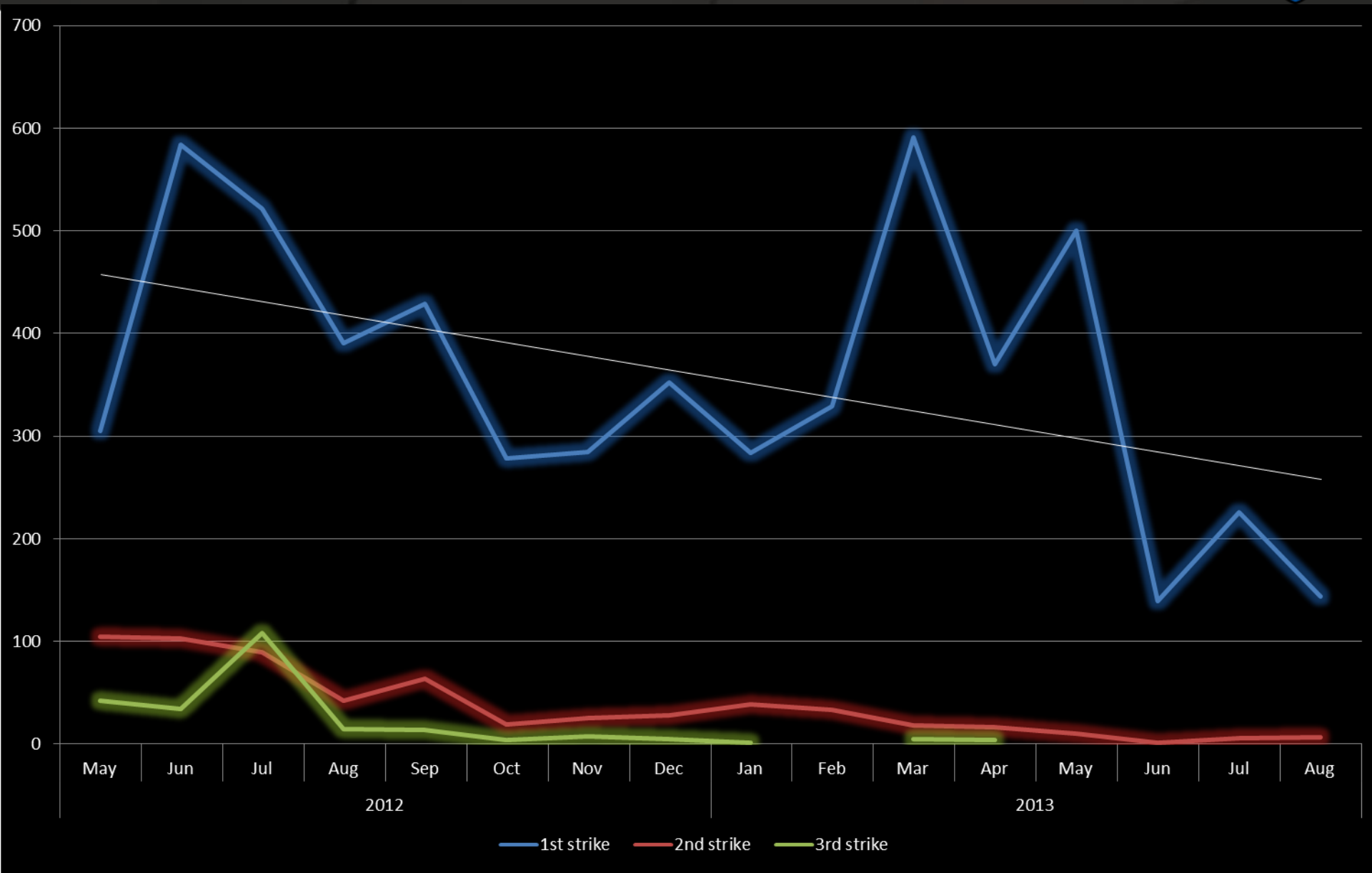
# Risk profile

- Use the crunched data to detect botting
  - Crunch available data for different patterns
  - Lots of markers contribute
  - Adjustable thresholds for detection/aggressiveness.

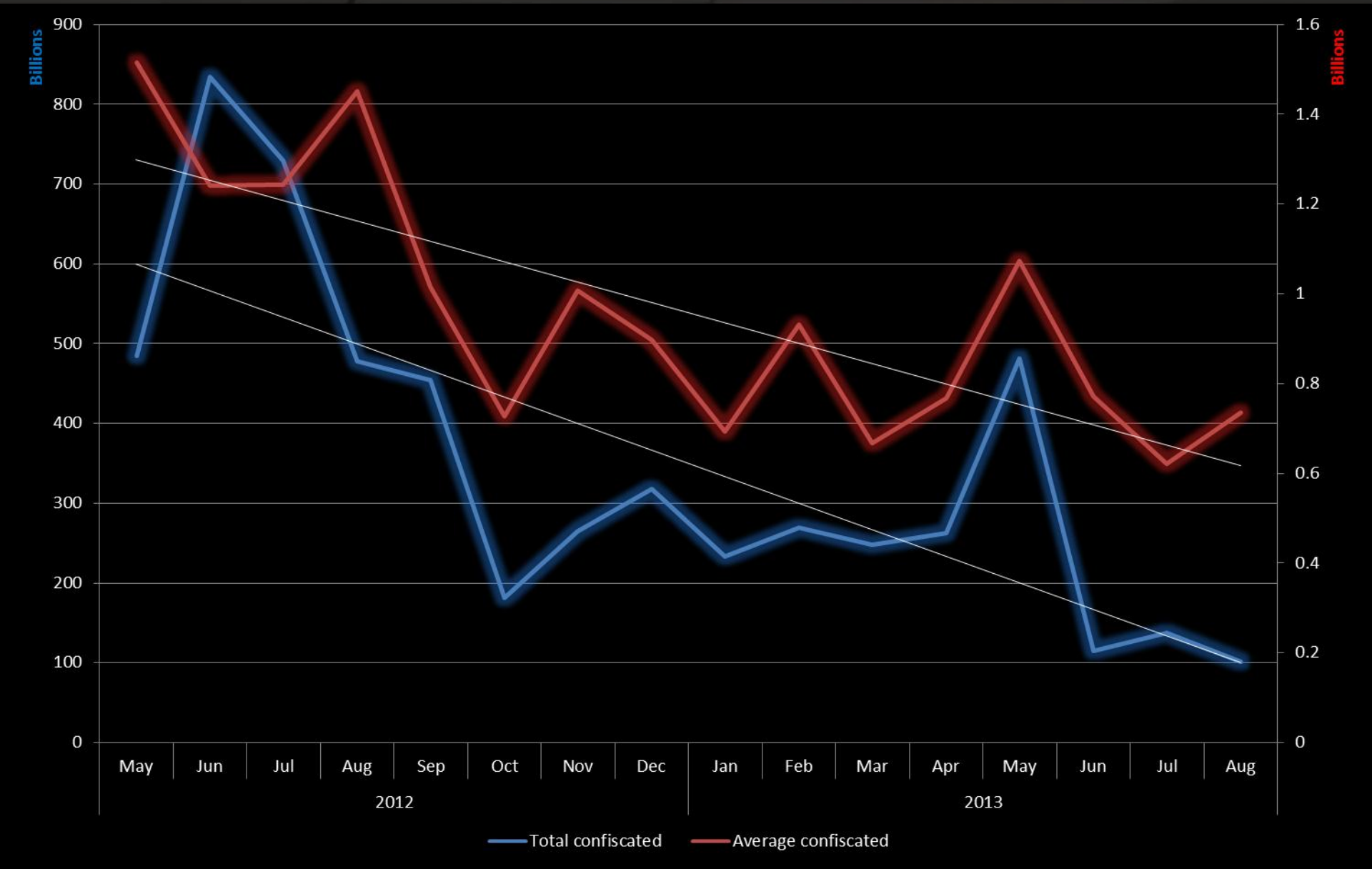
# Punishments

- Our first policy aimed to make players play legit:
  - 1st strike – 14 day ban
  - 2nd strike – 30 day ban
  - 3rd strike – Permanent ban
  - Exploits, client modification, RMT – Permanent ban
- After a while, that was no longer a concern:
  - 1st strike – 30 day ban
  - 2nd strike – Permanent ban
  - Exploits, client modification, RMT – Permanent ban
- Automated removal of gains implemented in May 2012

# Detection rate



# ISK Confiscation



# This has fallout....

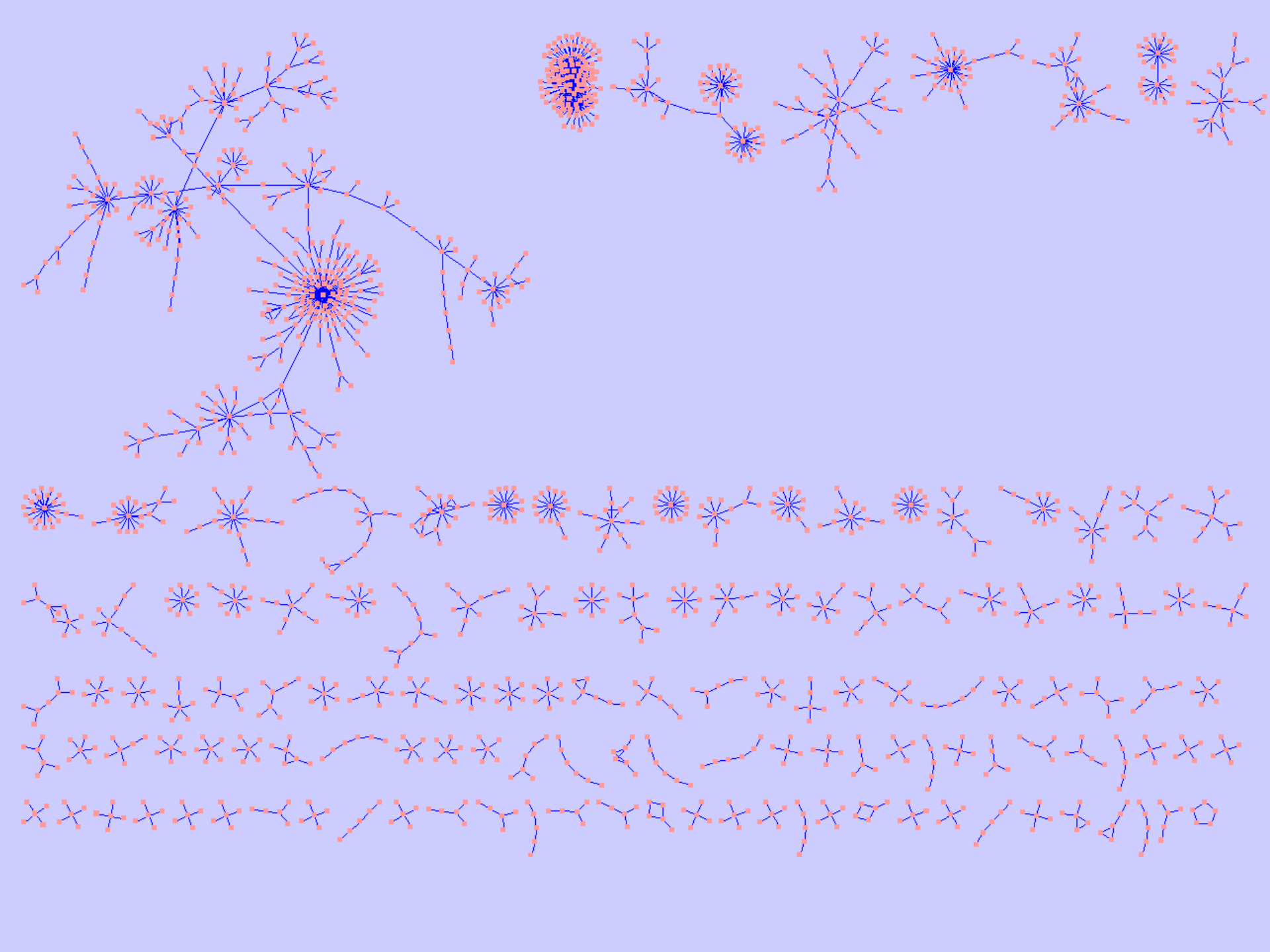
# STEP 2 – MAKE MONEY LAUNDERING AND RMT SALES MORE RISKY

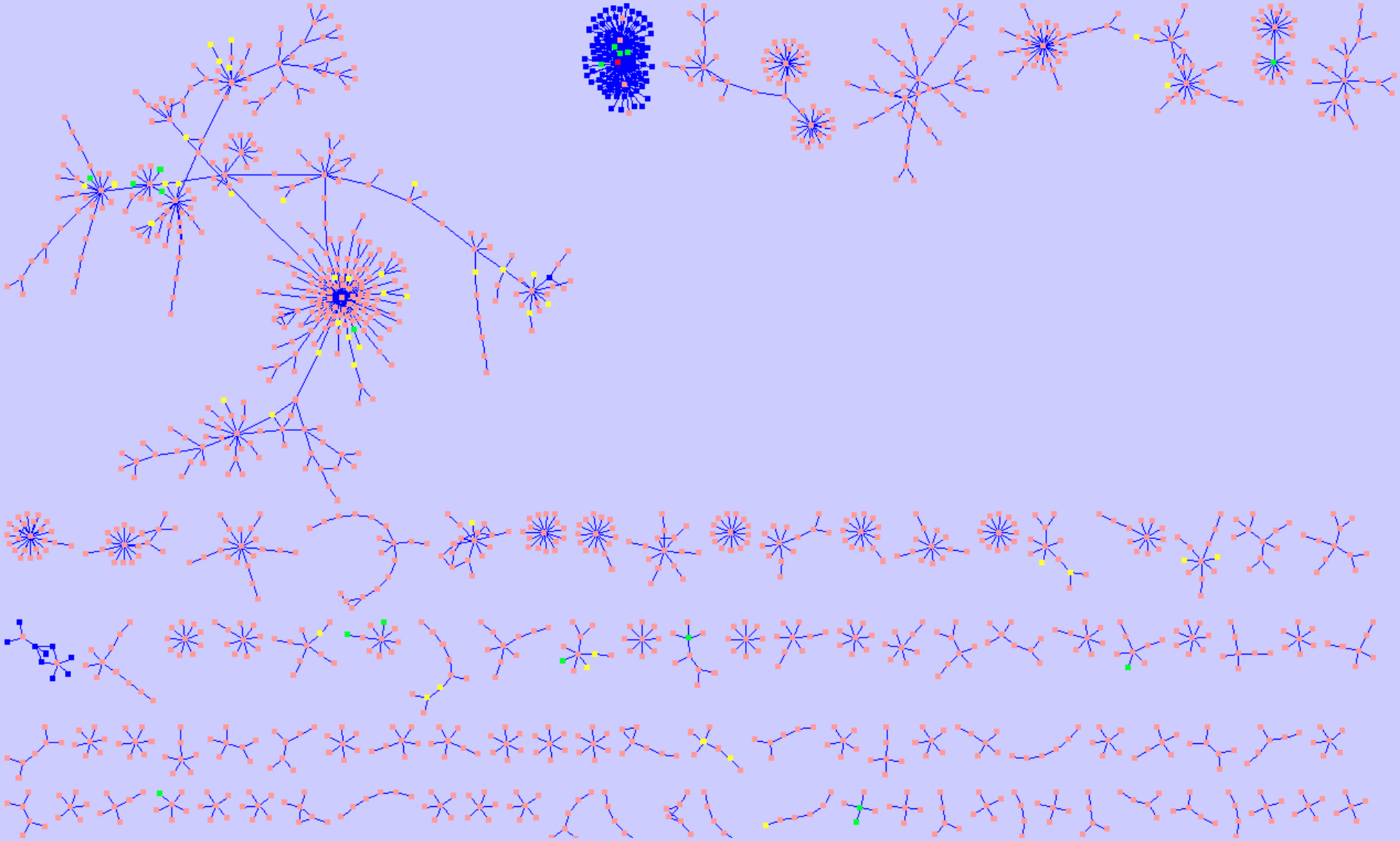
# Goals

- Track ways in which money is laundered
- Find ways to catch RMT as it occurs

# Step 2.1 – Graph analysis

- The more you do in EVE, the more data you create
- Real players are inherently noisy/unpredictable
  - RMTers are not noisy
- By looking at intersection properties on an interaction graph, we can do things!
- We can take the data we have and represent it as nodes and edges(interactions)
- We can add extra data on top of it to enhance clarity
- Decent tooling does exist
  - Maltego
  - Cytoscape

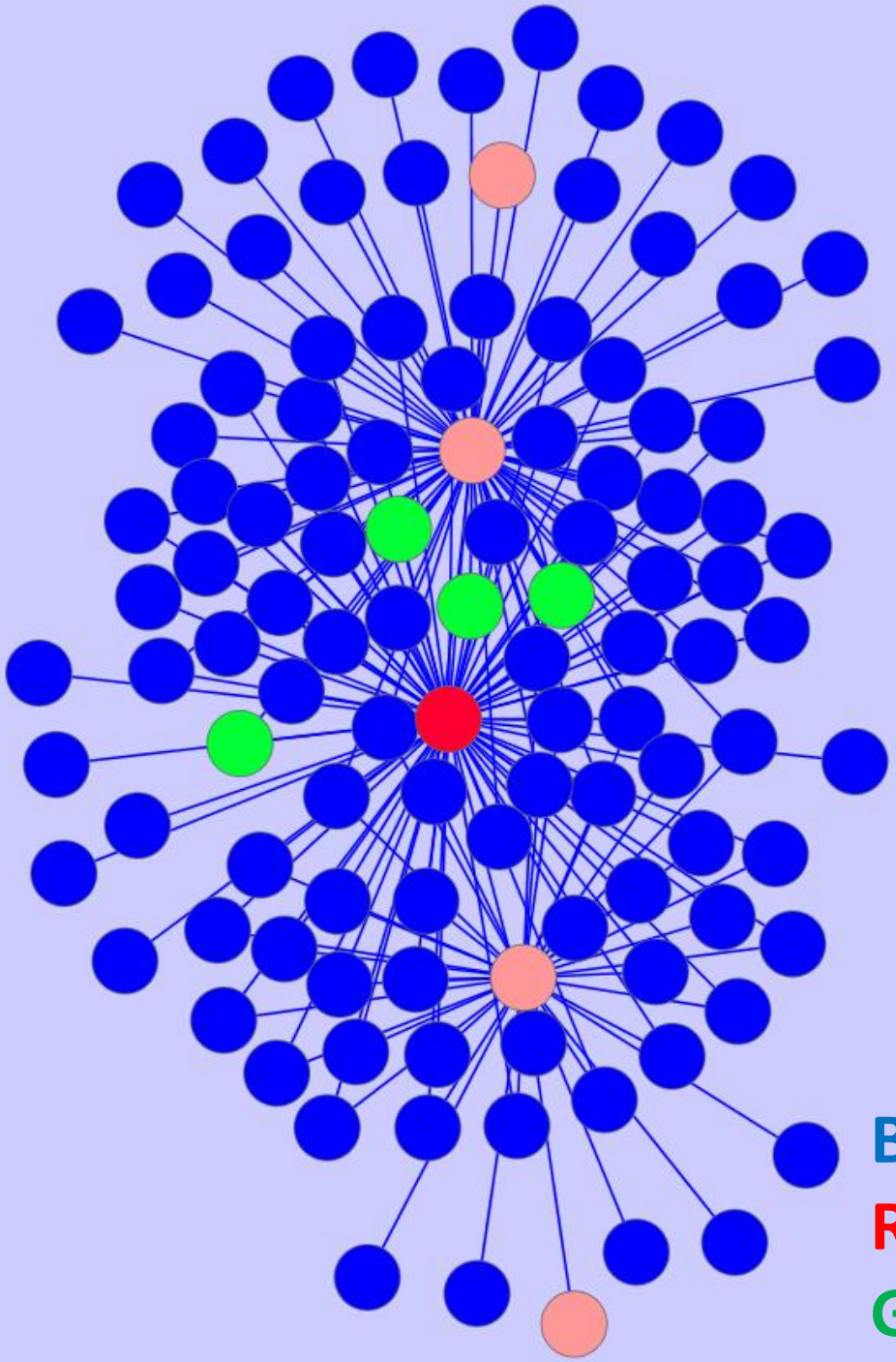




Blue = Reported bot

Red = Real Money Trader

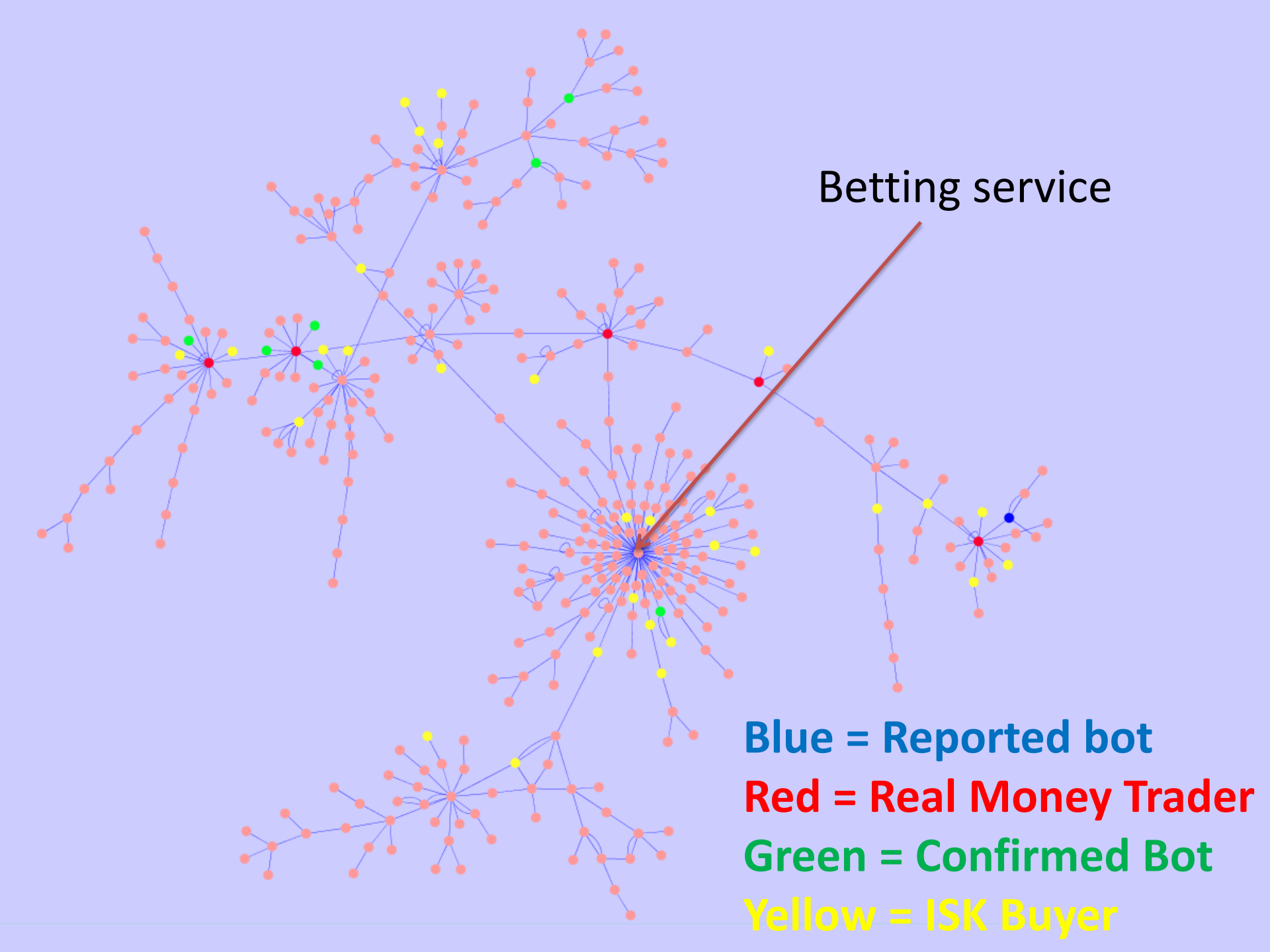
Green = Confirmed Bot

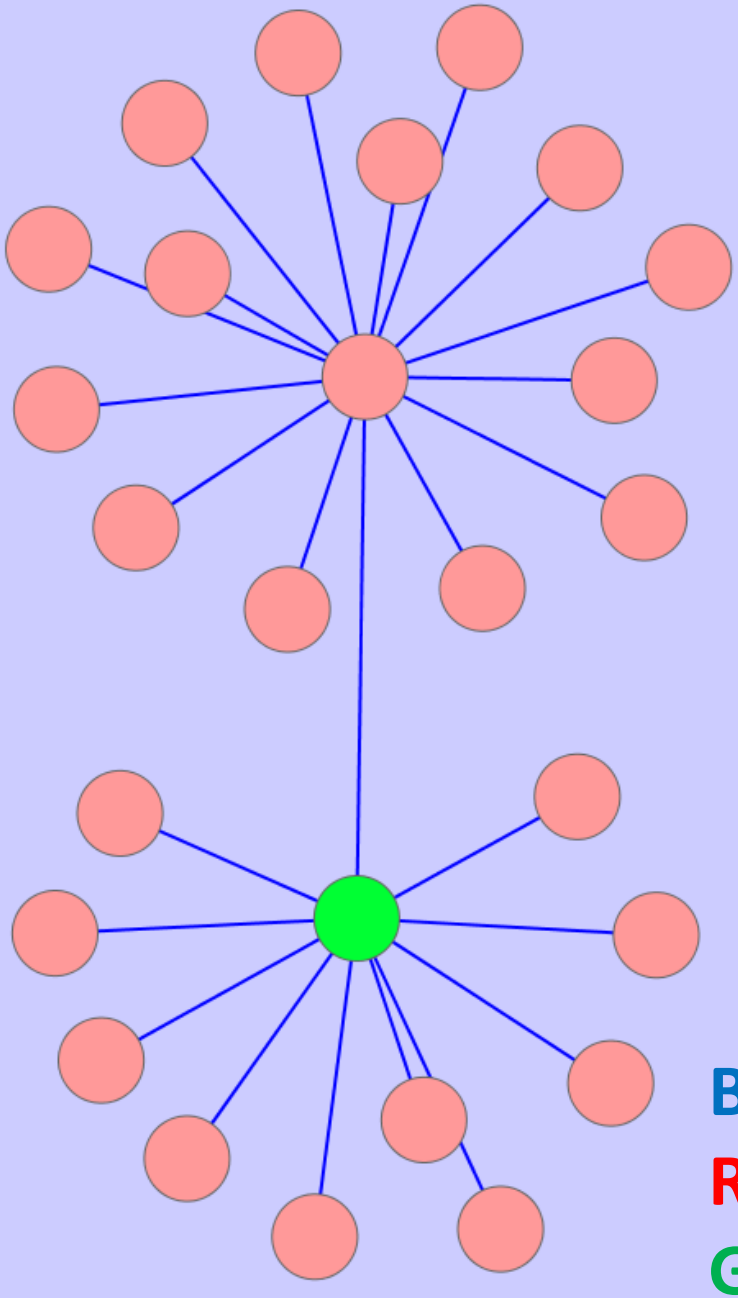


Blue = Reported bot

Red = Real Money Trader

Green = Confirmed Bot

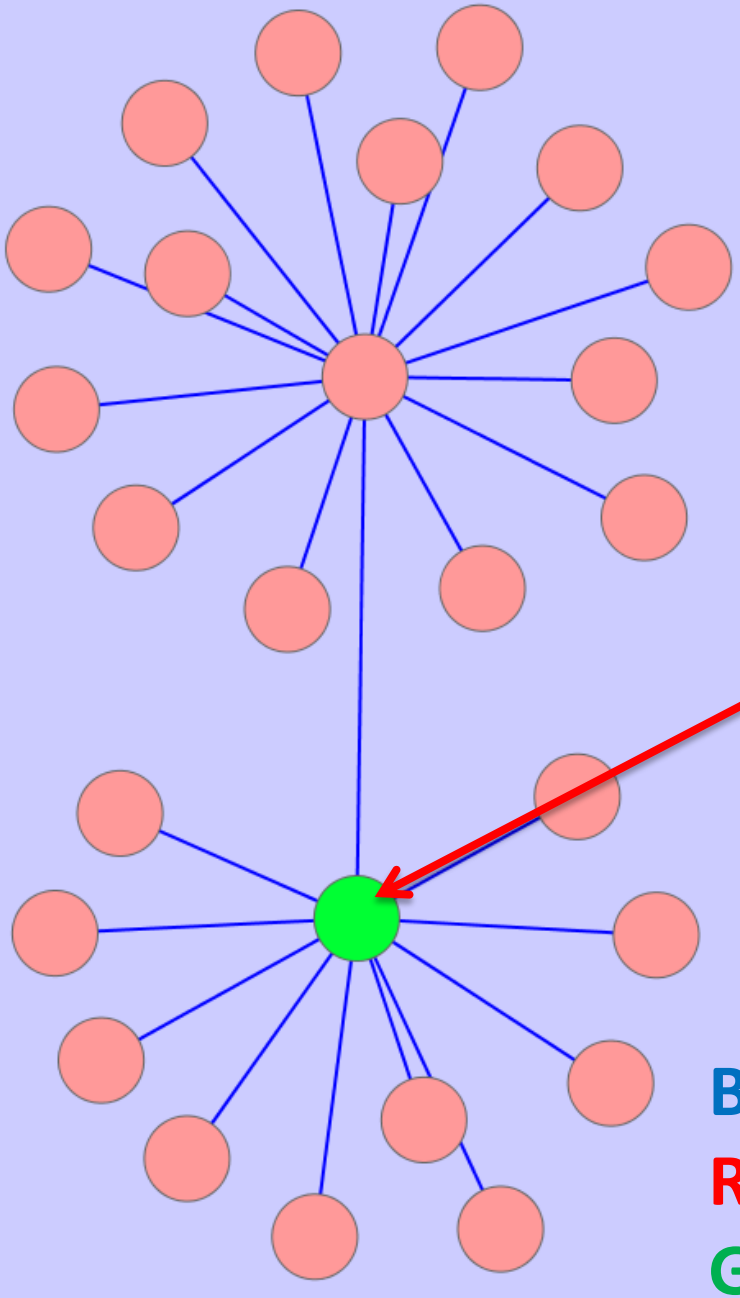

Betting service
Blue = Reported bot
Red = Real Money Trader
Green = Confirmed Bot
Yellow = ISK Buyer



Blue = Reported bot

Red = Real Money Trader

Green = Confirmed Bot




Blue = Reported bot

Red = Real Money Trader

Green = Confirmed Bot

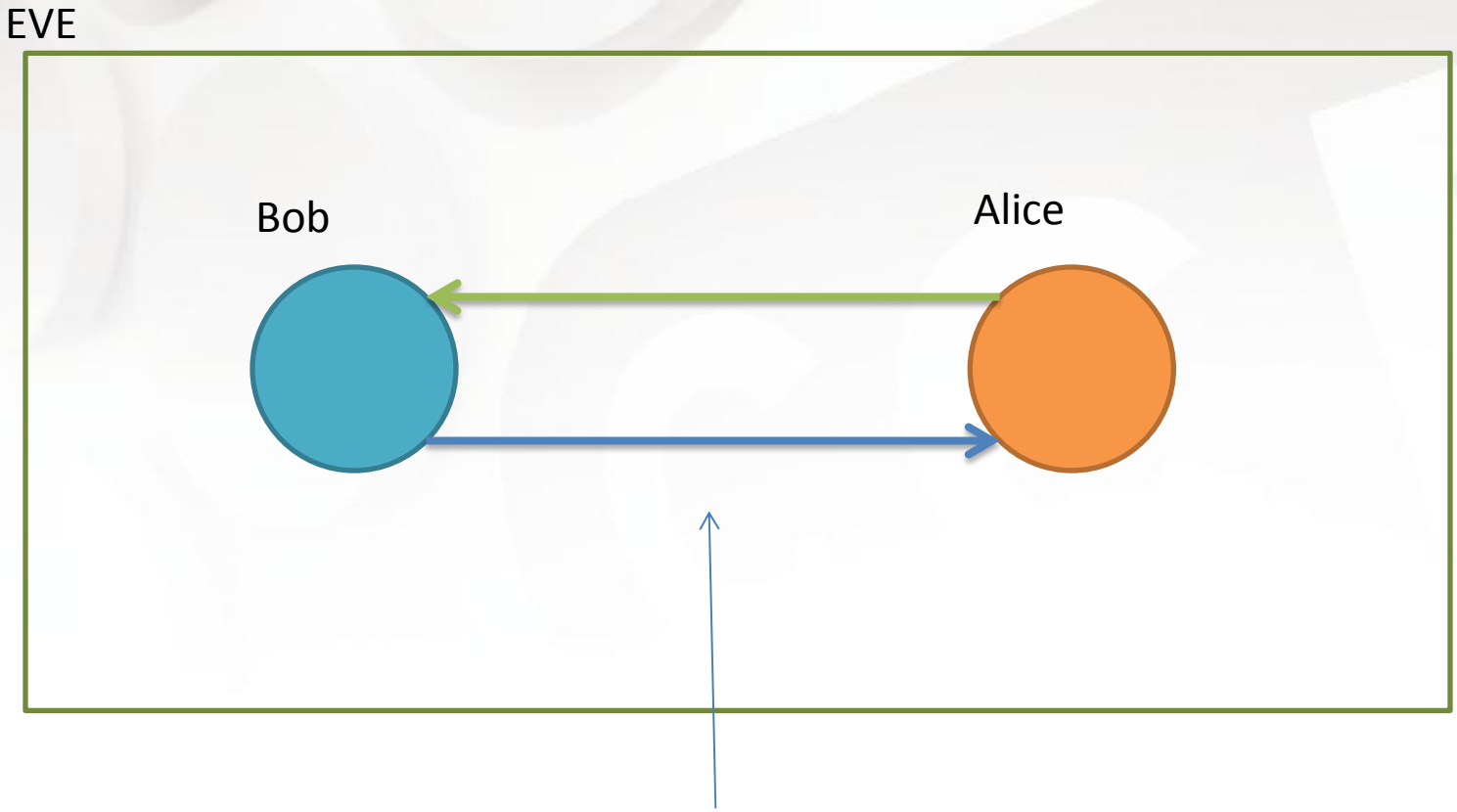
# What we learned

- Trying to hide creates signal
- We can use graphs to do manual anomaly detection
  - But you need to know what data to look at

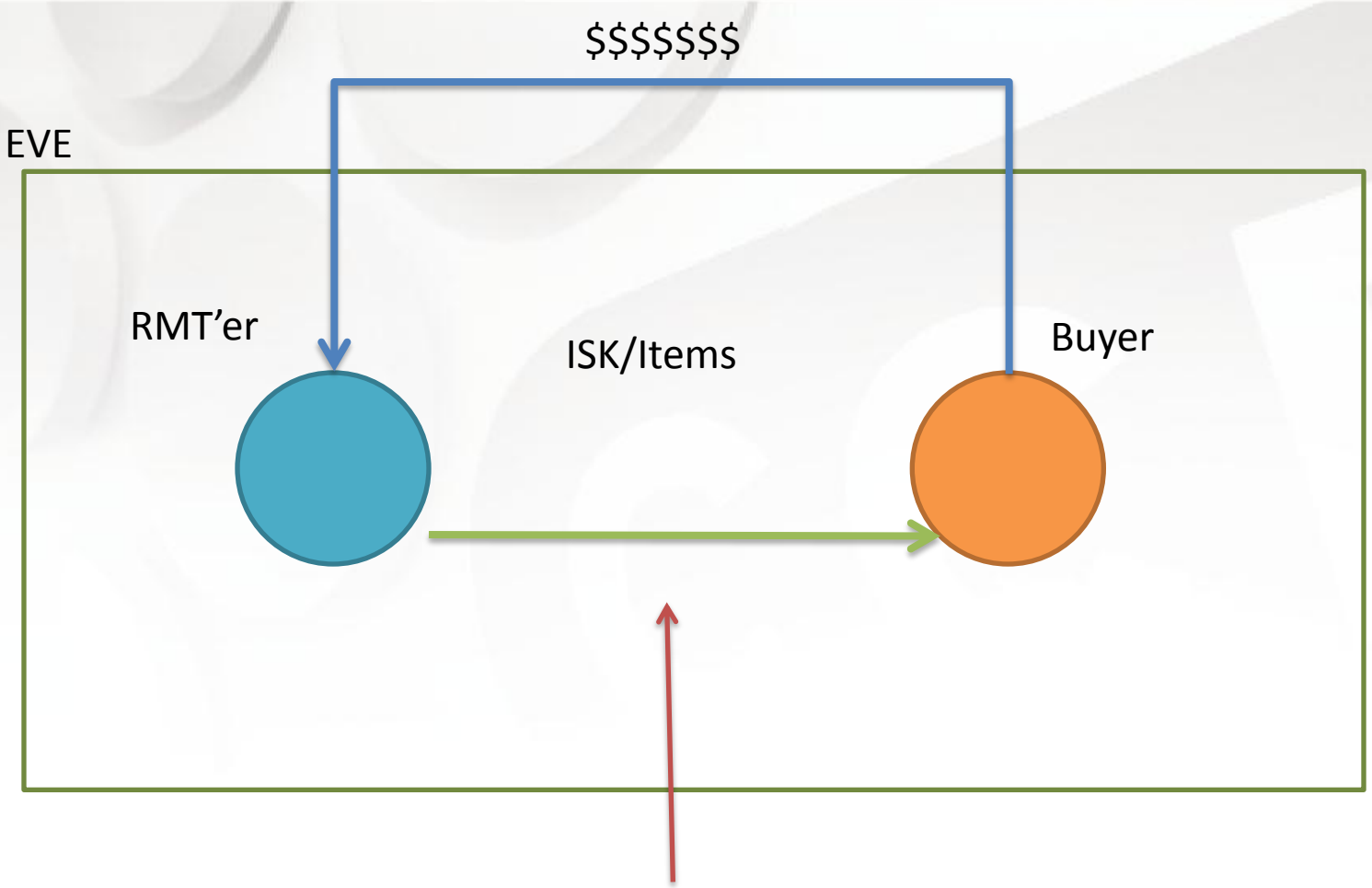
# Step 2.2 – Identify asymmetric relationships

- Or in other words, identify the ways they launder money
- It sticks out like a sore thumb
- Again, normal players are inherently noisy, bad guys creates more uniform noise, turning it into signal

# Normal relationship



# Asymmetric relationship




Give and take, but we don't see half the transaction, making it asymmetric


# STEP 3 – MAKE CLIENT MODIFICATION MORE RISKY

# Client modification detection

- A technically harder/impossible problem
- You inherently can’t trust code running on a remote client
- How can you be sure it’s your code running?

# Approach

- We tried some ways to make it stop
  - They only lasted a number of hours
- If you can't prevent it, detect it
- Raise the barrier to entry for python injection

# Client monitor

- By sending a client challenges we can catch low-hanging fruit
- We can push random noise to the client
- And we can push signatures

# Signatures

- Approach
  - Based on reverse engineering of known bad software
  - When a signature triggers, it gets logged
  - Somebody manually investigates the result
  - Consider it a dumb AV for our platform
- Limitations
  - We can’t write signatures for everything
  - We do not want to leave our own process

# Results

- We banned ~3000 paying accounts as a result
- We made some cheating software go behind a paywall
- We killed a specific hack commonly used

# Conclusions & Endgame

- Next step: Improve account security to prevent account hacking better
- We were able to reduce problems to make them more manageable in the mid-term
- We were able to show more rapid and instantaneous effectiveness
- But the issue remains a constant and mildly escalating arms race
- Work continues to progress towards end goals
  - Move the behavior into the “underground”
  - Drive up cost of business for RMT
  - Decrease profitability of botting


# Questions!

Charlie Eriksen

@CCP_Stillman / @charlieeriksen

charlie@ccpgames.com / charlie@ceriksen.com