EVE®

FANFEST 2014

EVE FANFEST SPONSORS:

intel®

NVIDIA® GEFORCE® GTX THE WAY IT'S MEANT TO BE PLAYED™

ICELANDAIR

twitch

Gull

HIGHWINDS GAME DELIVERY NETWORK

IBM

NÝHERJI

sensa

SMIRNOFF

globalcollect payments. knowledge. growth.

musterbrand

EVE ONLINE

EVE DUST 514®

EVE VALKYRIE™

CCP®

From Evidence to Bans

CCP Security

EVE FANFEST 2014

CCP Security :: Who we are

CCP Security

Team Security

InfoSec

CCP Grimmi

Security Specialist

- Game Master, Customer Support Specialist and Payment Fraud Guardian since 2003
- With CCP since 2003
- Topics: Account Security, Payment Fraud, Anti-RMT Squad

CCP Peligro

Security Specialist

- Game Master 2006-2007, Internal Affairs 2007-2012, Team Security since 2012
- With CCP since 2006
- Topics: Game Data Analytics, Anti-RMT Squad

CCP Random

Security Engineer

- IT-Security Professional since 2008
- With CCP since 2014
- Topics: Infrastructure Security and Secure Development, Incident Handling

CCP Bugartist

Director of InfoSec

- Information-Security Professional since 2003
- With CCP since 2013
- Topics: Security Processes, Concepts and Guidelines, Wizard, Enablement

CCP Blofeld

IT Director

- IT Professional since 1995
- With CCP since 2012
- Topics: IT Strategy, Managing Vendor relationships, Budget and the People in VW Operations and Office IT

Today’s Agenda

- Introduction
- Updates
  - InfoSec
  - Team Security
- Security Tips & Tricks
- Roadmap

This order will not be followed, really!

- Q&A – Please join our Round Table*

*Actually we cannot guarantee that the table will be round

InfoSec

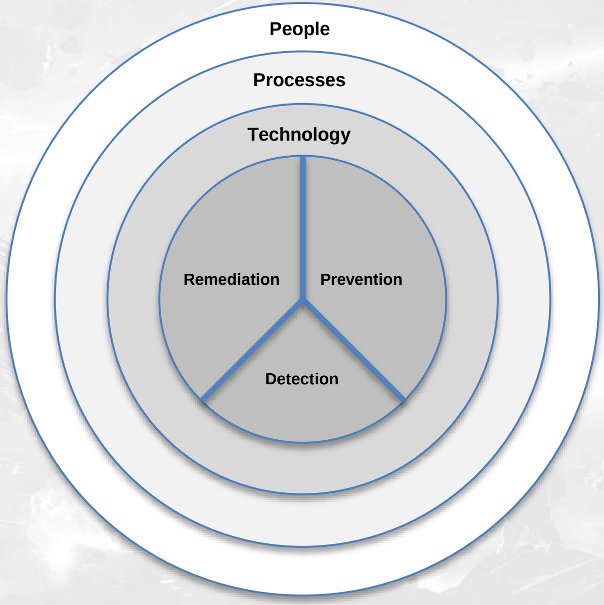
InfoSec :: Hot Topics

- Improving Overall Security
  - Improving Security and Risk Management
    - E.g. Enhancing Intrusion Detection and Incident Handling
- Fighting Threats
  - Distributed Denial of Service Attacks

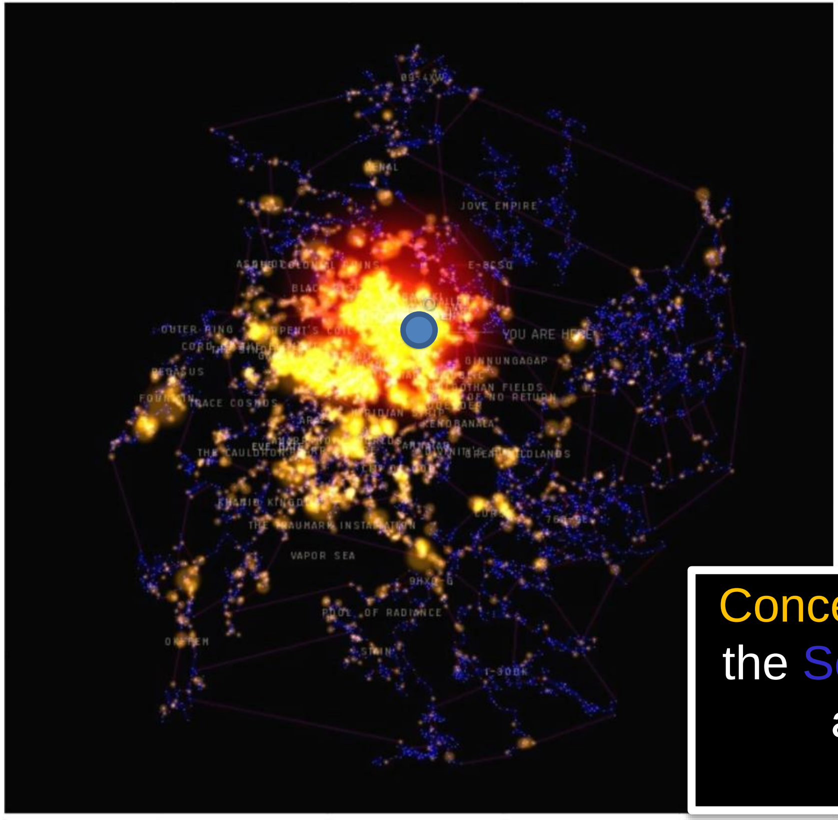
InfoSec :: Improving Security

Security and Risk Management

- Restructuring the way on how security is being applied
- Providing clear service offerings to all our departments
- Aligning processes and metrics throughout all of CCP



What is a DDoS Attack?



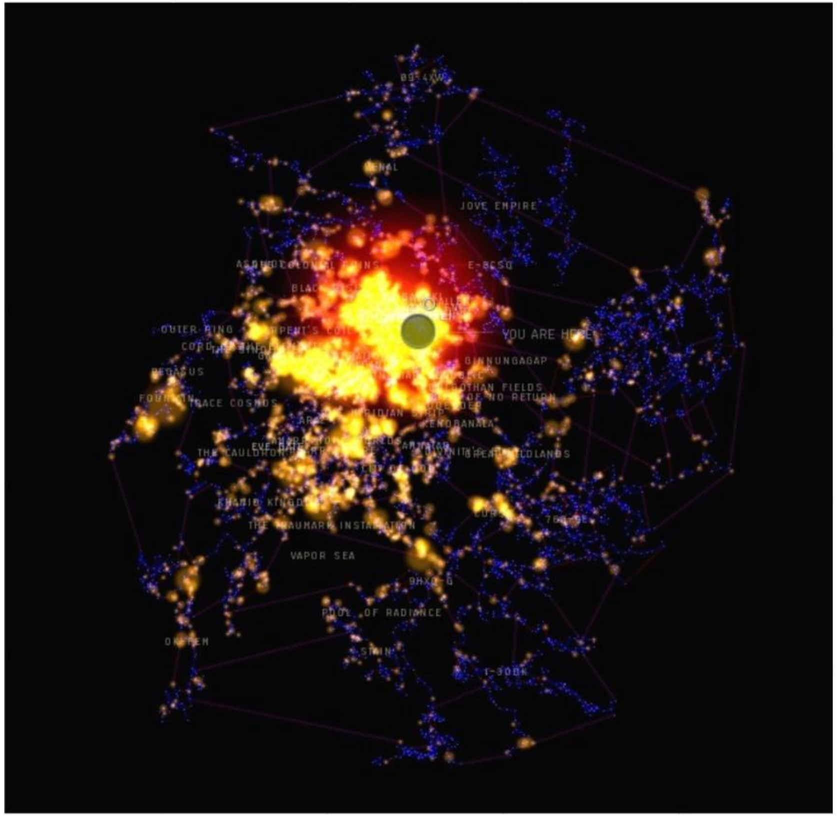
Virtual situation equivalent:

1. Many players warp to one hub, e.g Jita
2. Routes are used to overload the target gates
3. Target appears to be closed (overcrowded)

The network situation appears comparable.

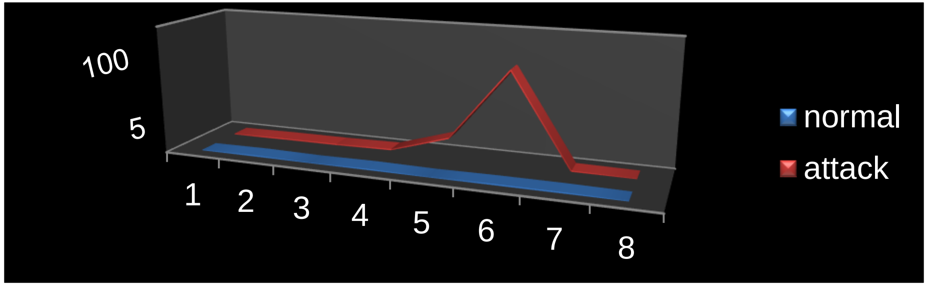
Concentration of **ships** present in the Solar Systems around Jita on an „average weekend“.
Marked with ●

Netwok based DDoS Attacks

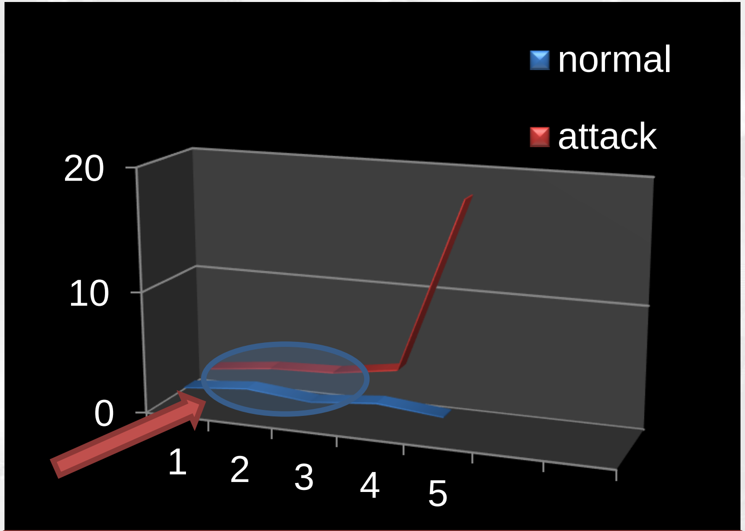


Anatomy of a network DDoS attack:

1. Direct (reflect) network traffic to the target
2. Routes (hops / jumps away) overload the target uplink
3. Target appears to be down (overloaded):



Early DDoS Detection

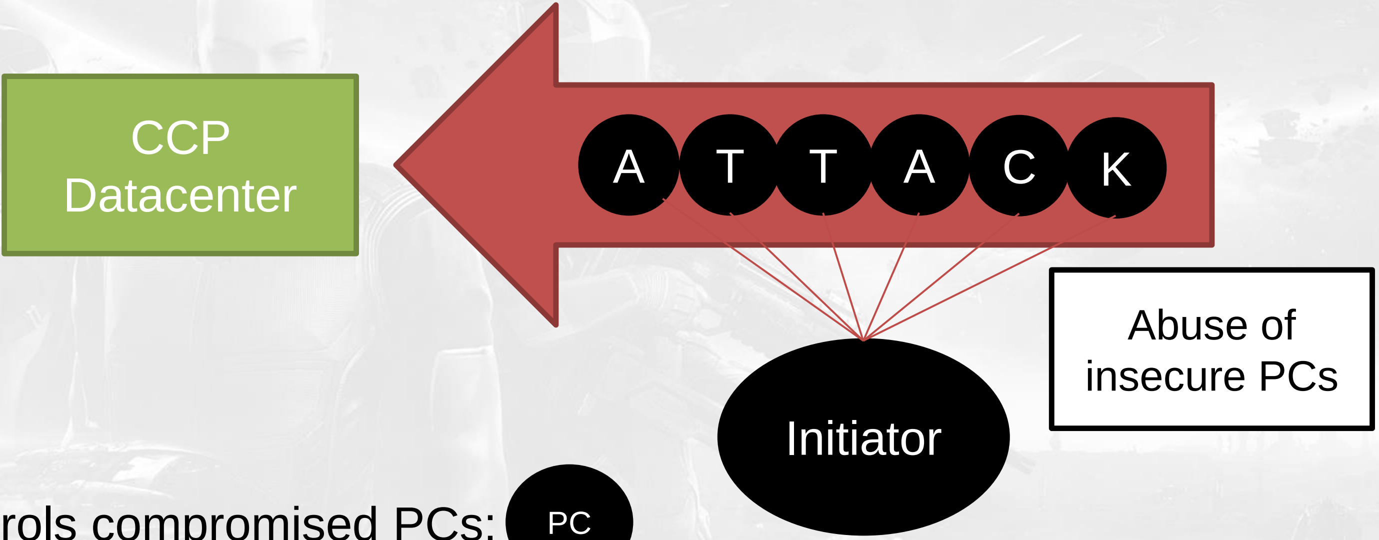


- **Detect early:**
  - Traffic anomalies
    - Composition
    - Patterns (IPs, Protocols)
- Prepare early:
  - Prepare network
  - Coordinate efforts

In 2014 we already faced over a dozen network DDoS attacks with upto 75 Gbit spikes

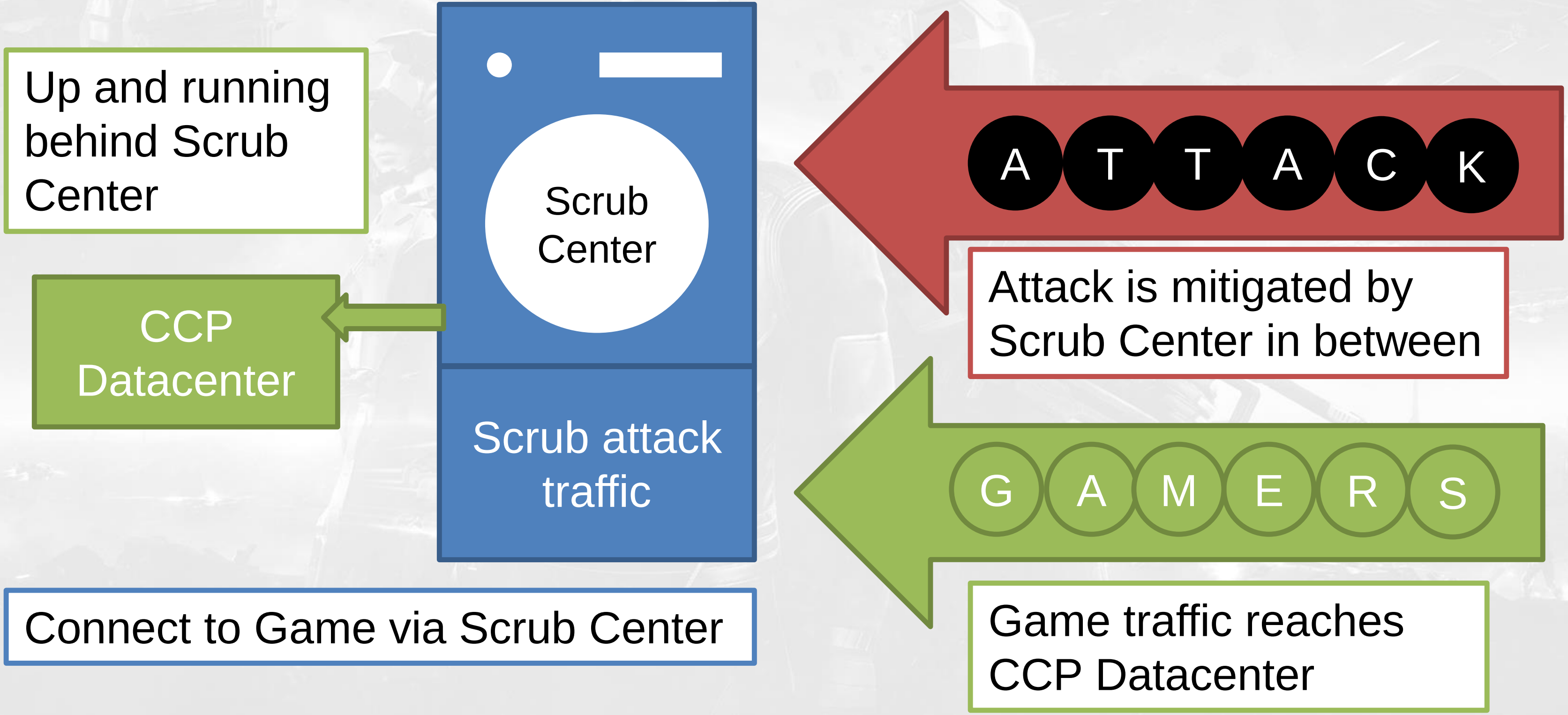
We improve our detection and mitigation capabilities and we are working on preventive measures

DDoS Mitigation Options



1. An Initiator controls compromised PCs: PC
2. Compromised PCs send attack traffic
3. CCP Datacenter detects initial pattern
4. CCP prepares mitigation

DDoS Mitigation Options



Up and running behind Scrub Center

CCP Datacenter

Scrub Center

Scrub attack traffic

ATTACK

Attack is mitigated by Scrub Center in between

GAMERS

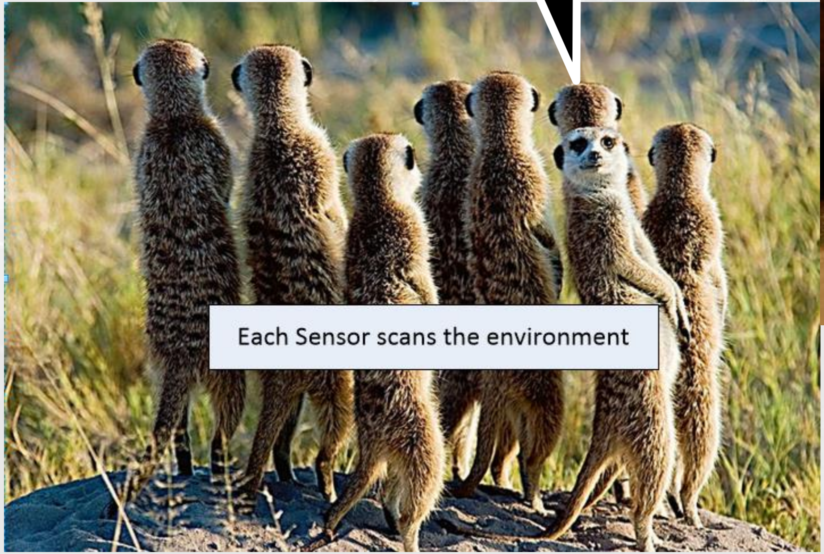
Game traffic reaches CCP Datacenter

Connect to Game via Scrub Center

Intrusion Detection Improvements

Security Feeds

Monitoring



Each Sensor scans the environment

Dashboard notifies and alerts

IDS Alert and Event Correlation

Retention

Team Security

Team Security :: Hot Topics

EVE FANFEST 2014

- Rules and Policy Updates
- Numb3rs
- EULA proof reading session

Two strike botting policy

We moved from a three strike policy on 15.03.2013.

Our current two strike botting policy:

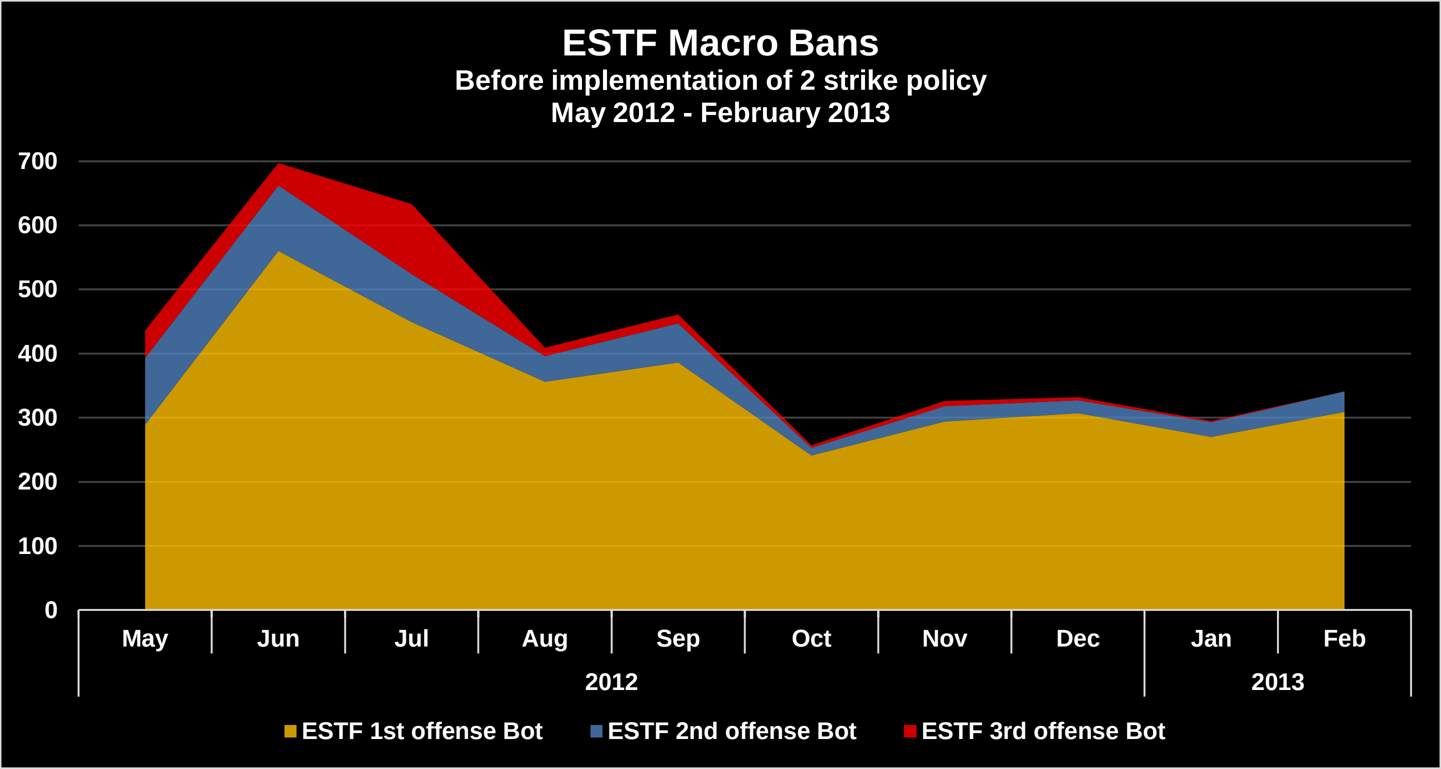
- 1st strike, 30 day ban, removal of botting proceeds, permanent character transfer-lock
- 2nd strike, Permanent ban

Client modification or involvement in RMT sales:

Zero tolerance, permanent ban on first offense.

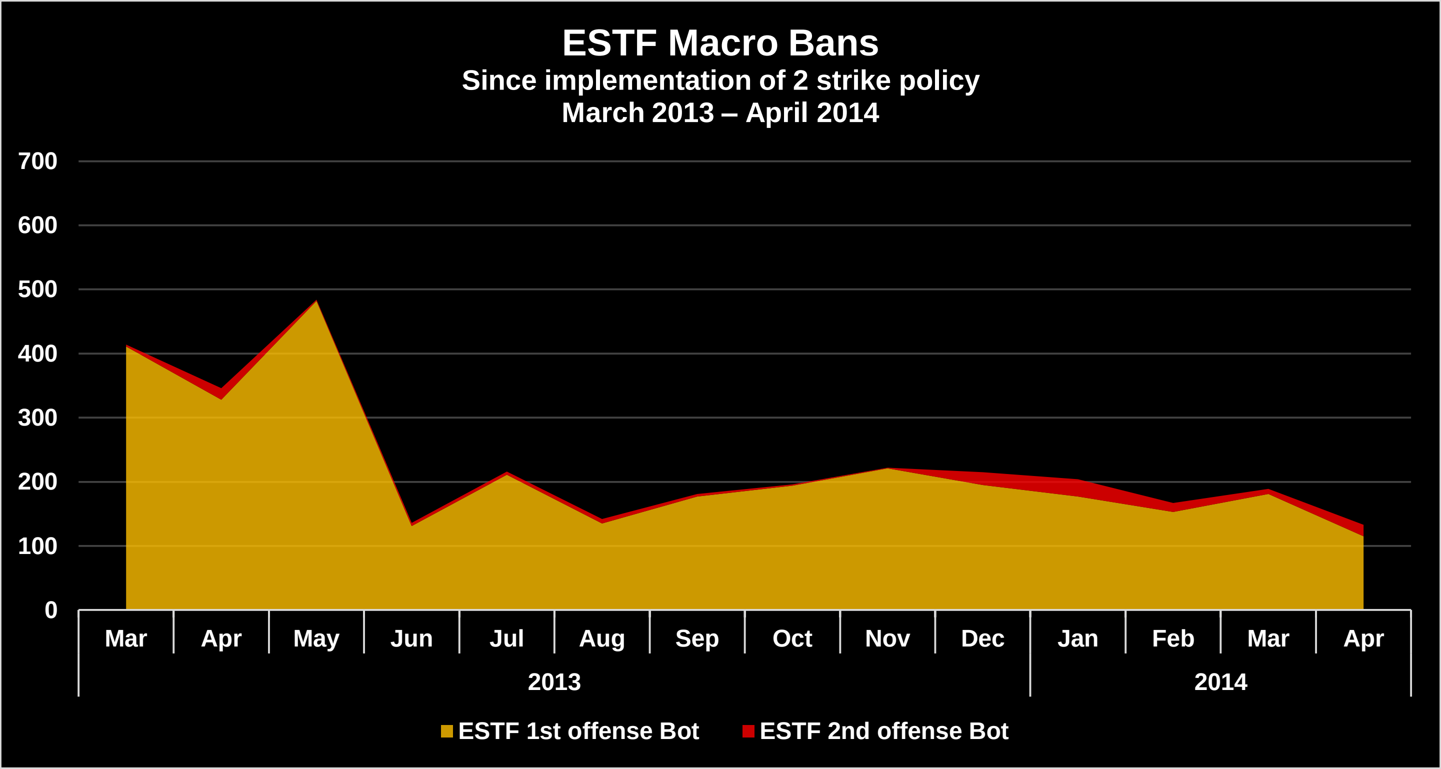
ESTF – Year of 2 strike botting policy

EVE FANFEST 2014

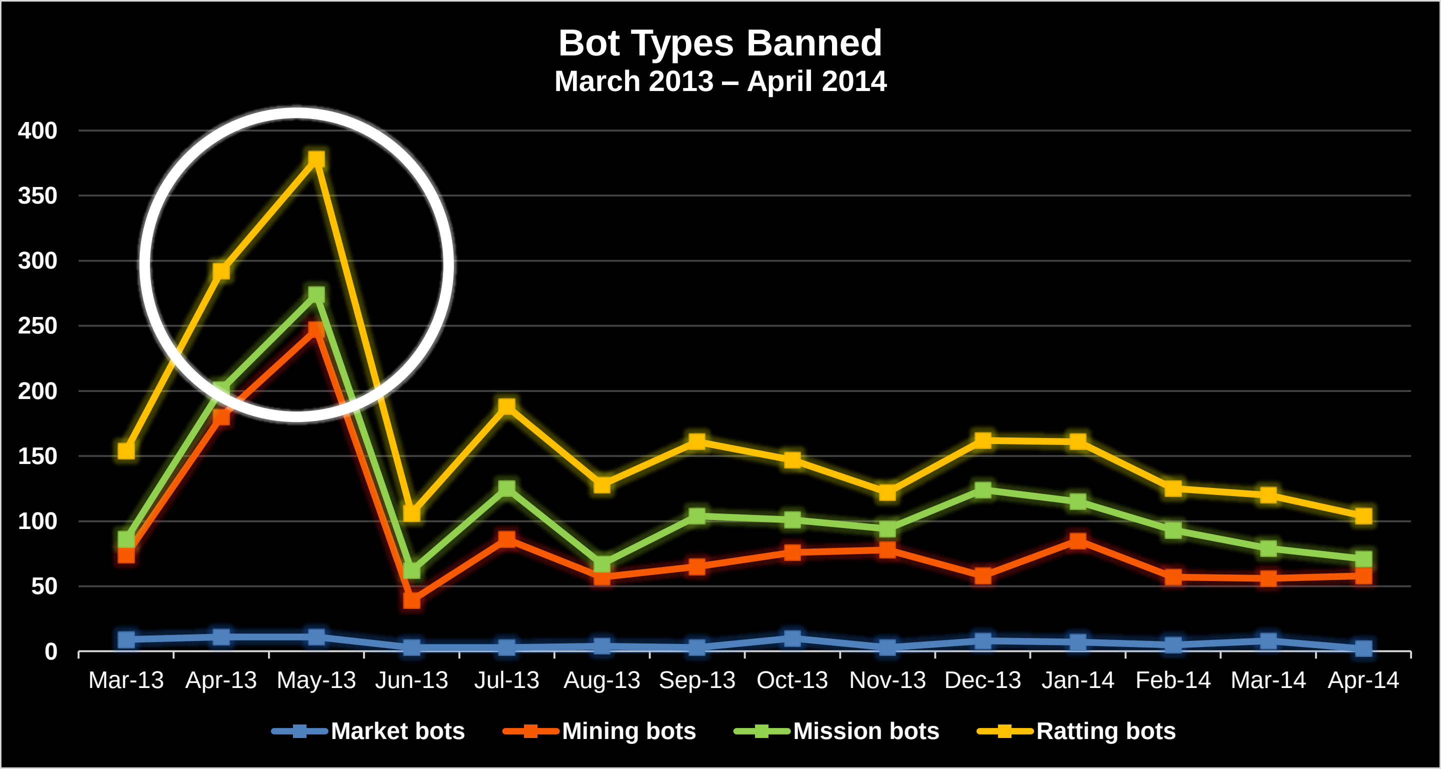


ESTF – Year of 2 strike botting policy

EVE FANFEST 2014



ESTF – Year of 2 strike botting policy



ISK Buyer policy

Our current 4-strike policy for ISK buyers is too lenient:

- 1st strike, ISK removed and a warning
- 2nd strike, ISK removed and 7 day ban
- 3rd strike, ISK removed and 30 day ban
- 4th strike, permanent ban

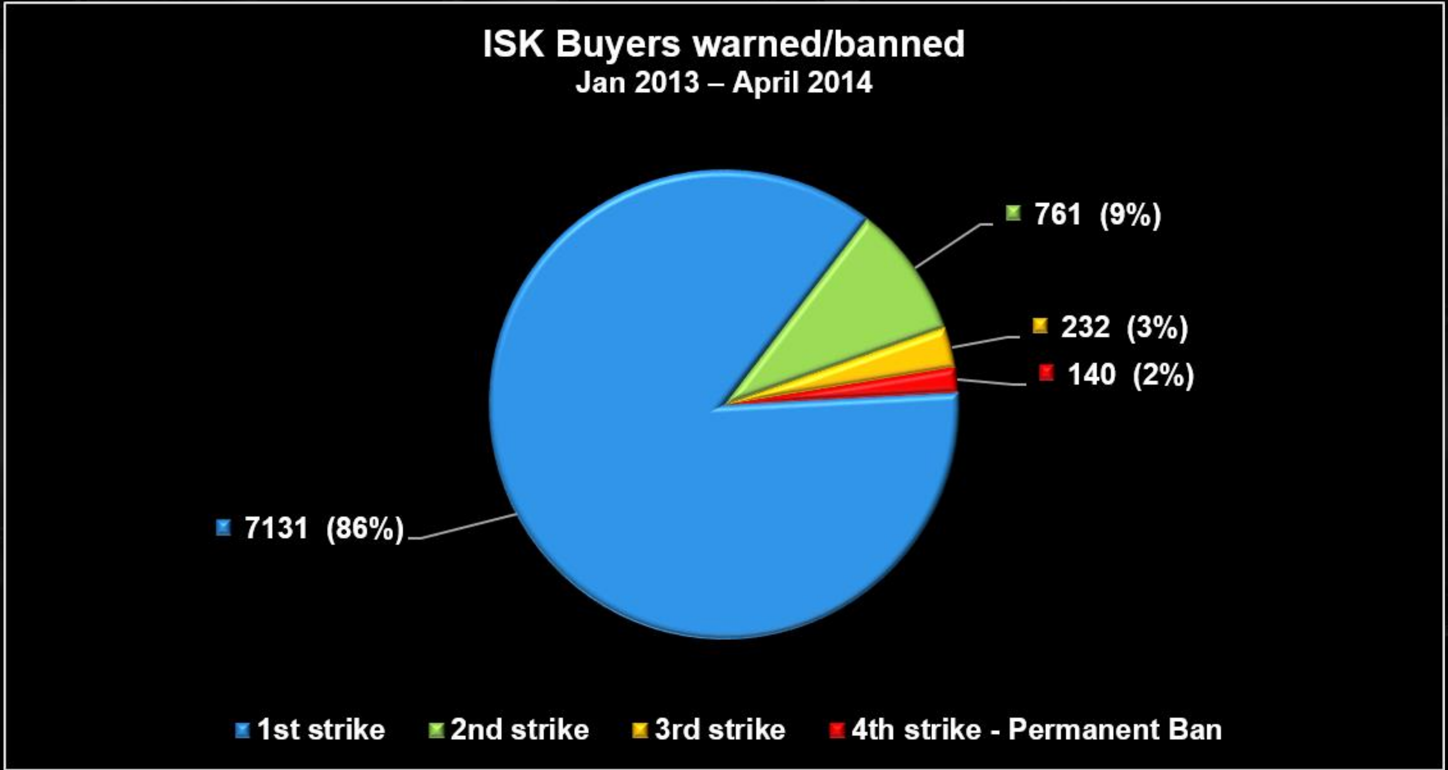
Three strike ISK Buyer policy

Going forward, our new policy for ISK Buyers will be:

- 1st strike, **7 days temporary ban** and removal of ISK
- 2nd strike, **21 days temporary ban** and removal of ISK
- 3rd strike, **PERMANENT BAN!**

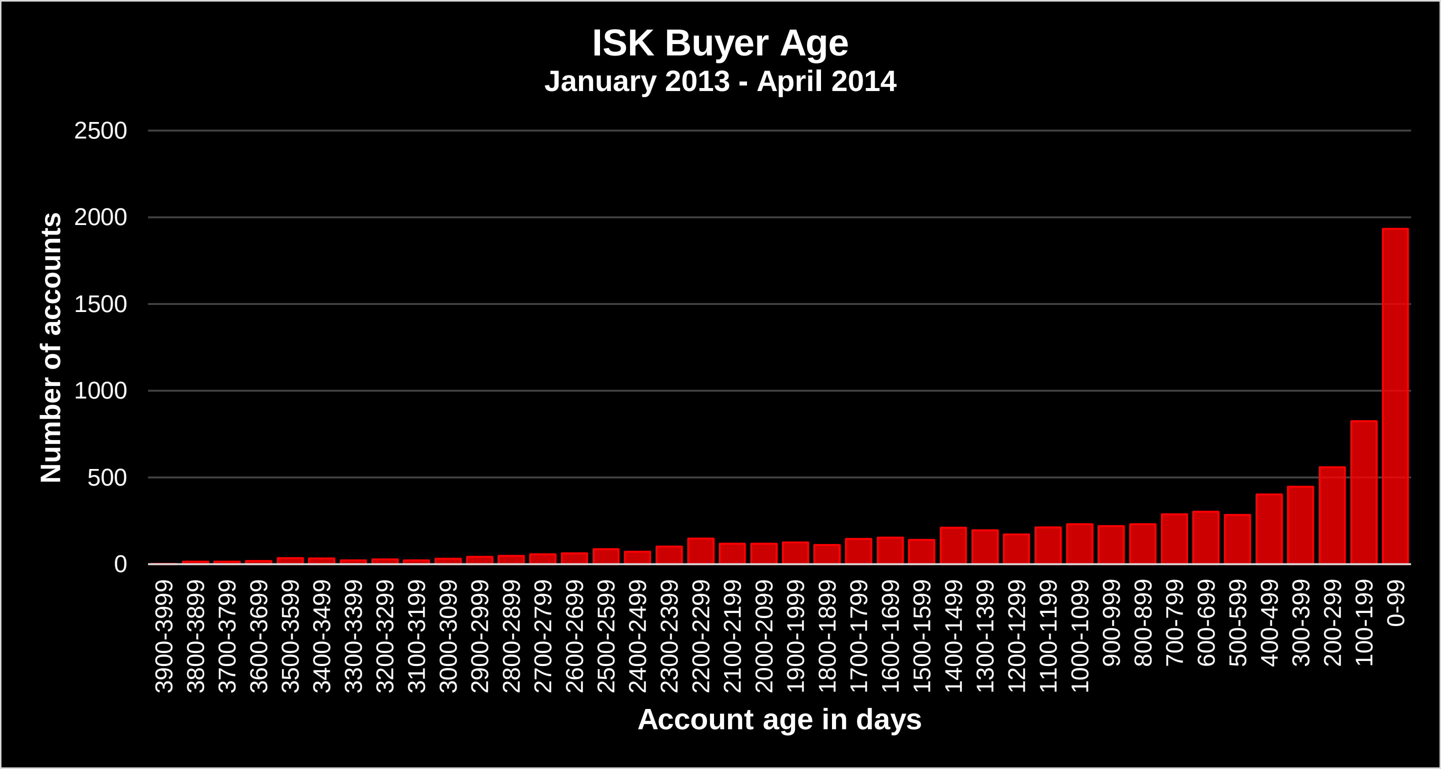
There will be a grace period; we aim to implement this policy in the next few weeks.

ISK Buyers


ISK Buyers warned/banned
Jan 2013 – April 2014
761 (9%)
232 (3%)
140 (2%)
7131 (86%)
🟦 1st strike
🟩 2nd strike
🟨 3rd strike
🟥 4th strike - Permanent Ban

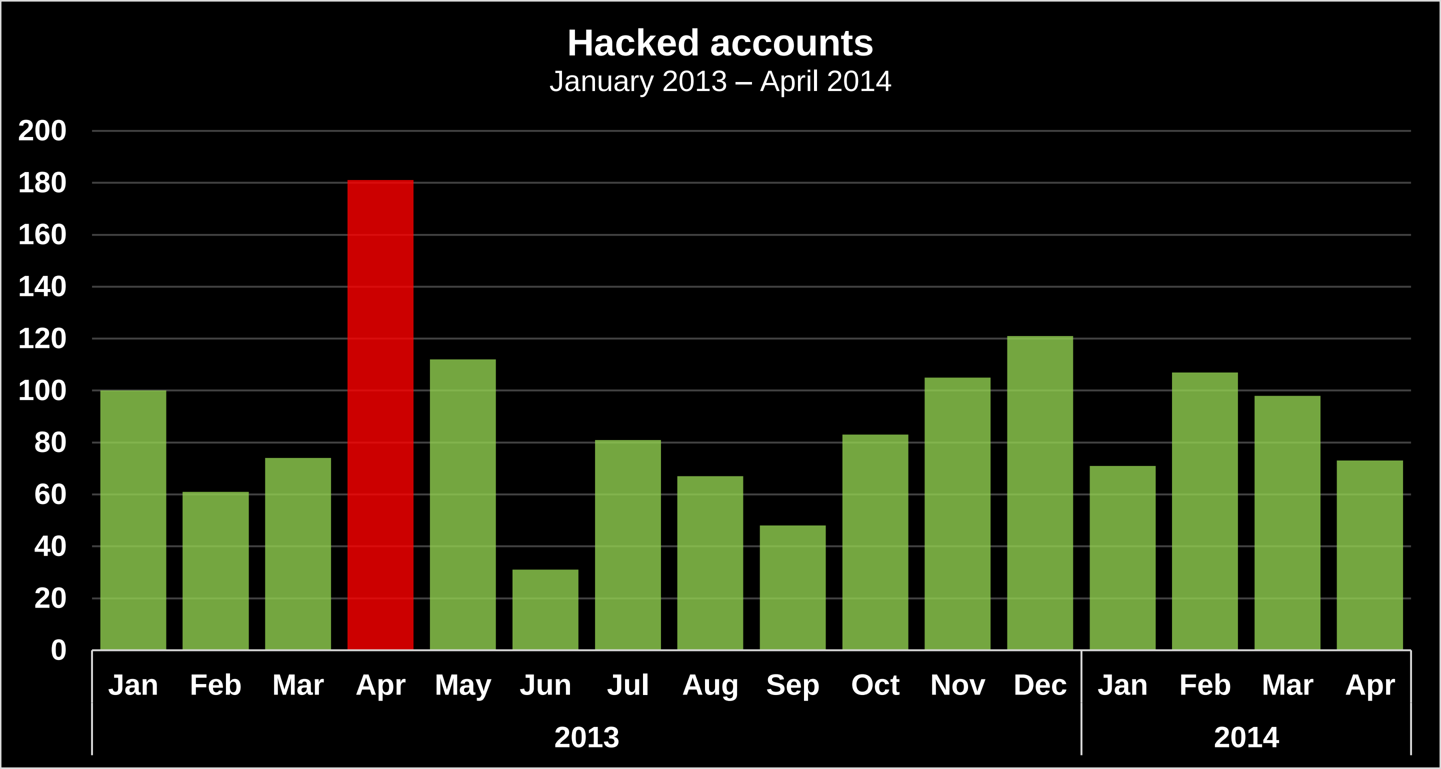
ISK Buyers

EVE FANFEST 2014

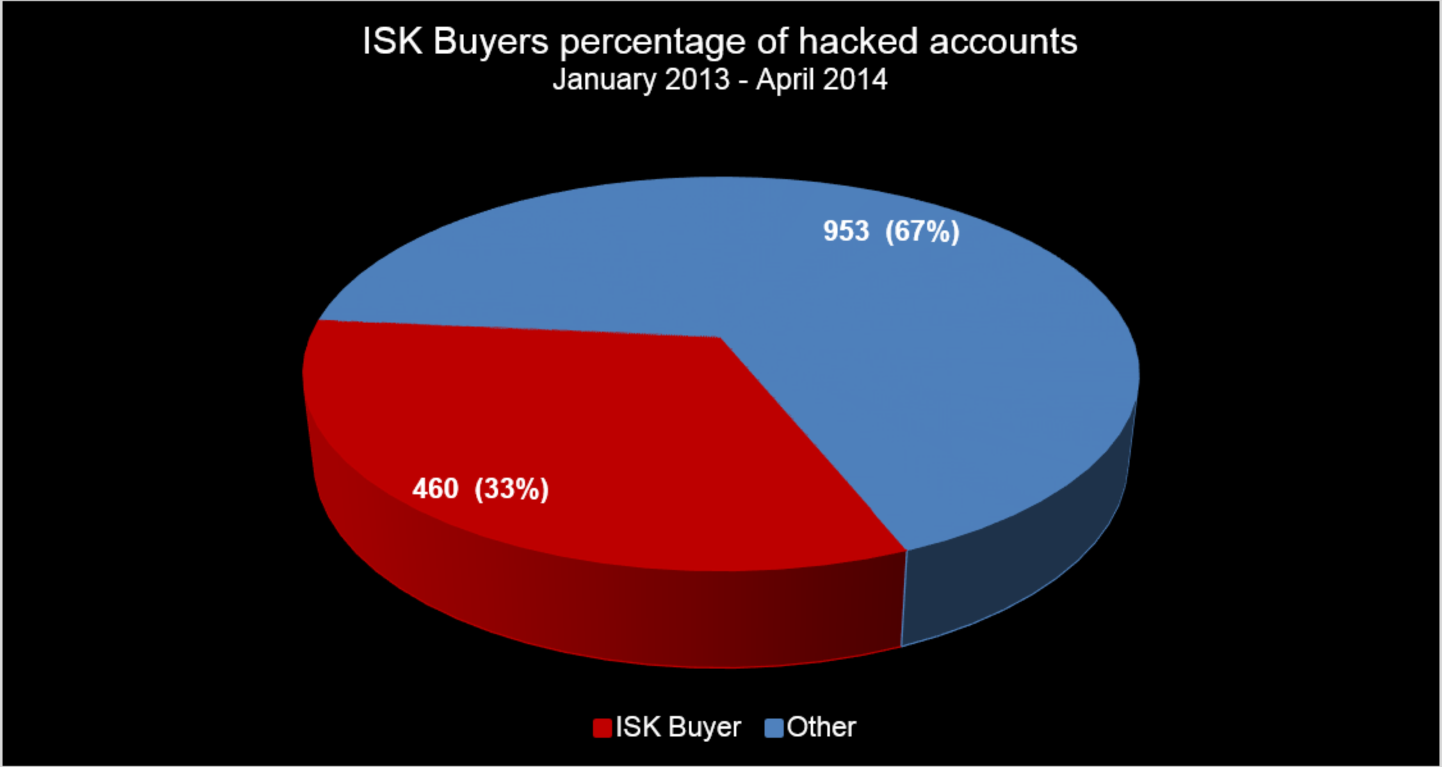


Account Security

Account Security

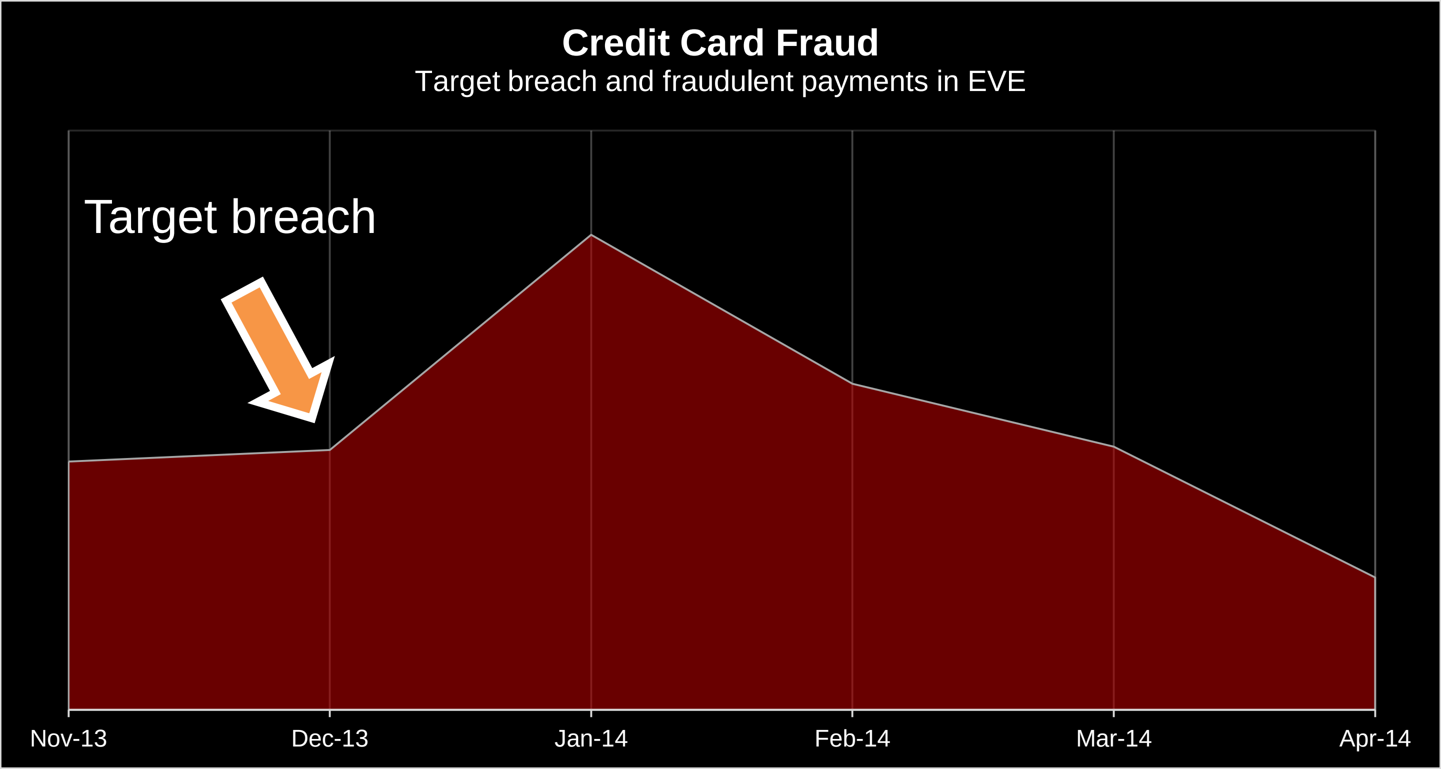


Account Security



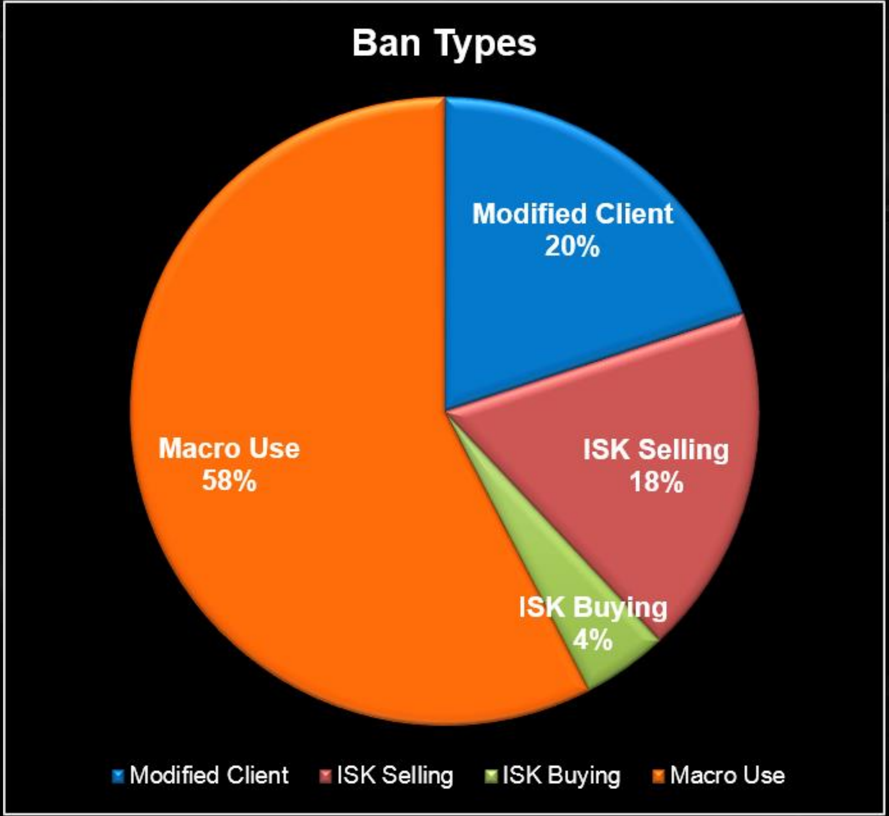
Account Security :: Payment Fraud

EVE FANFEST 2014



Team Security in Numb3rs

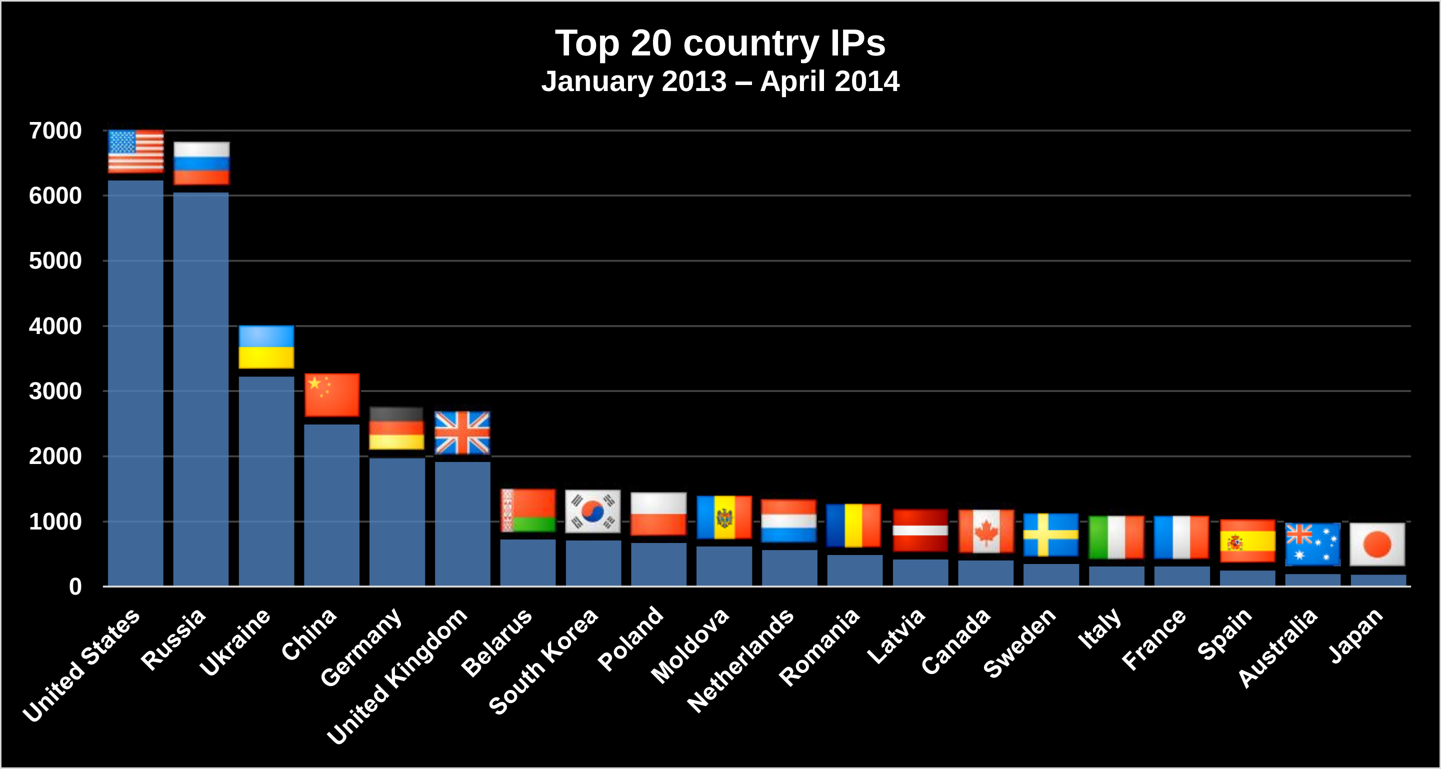
Types of bans issued



January 2013 - April 2014

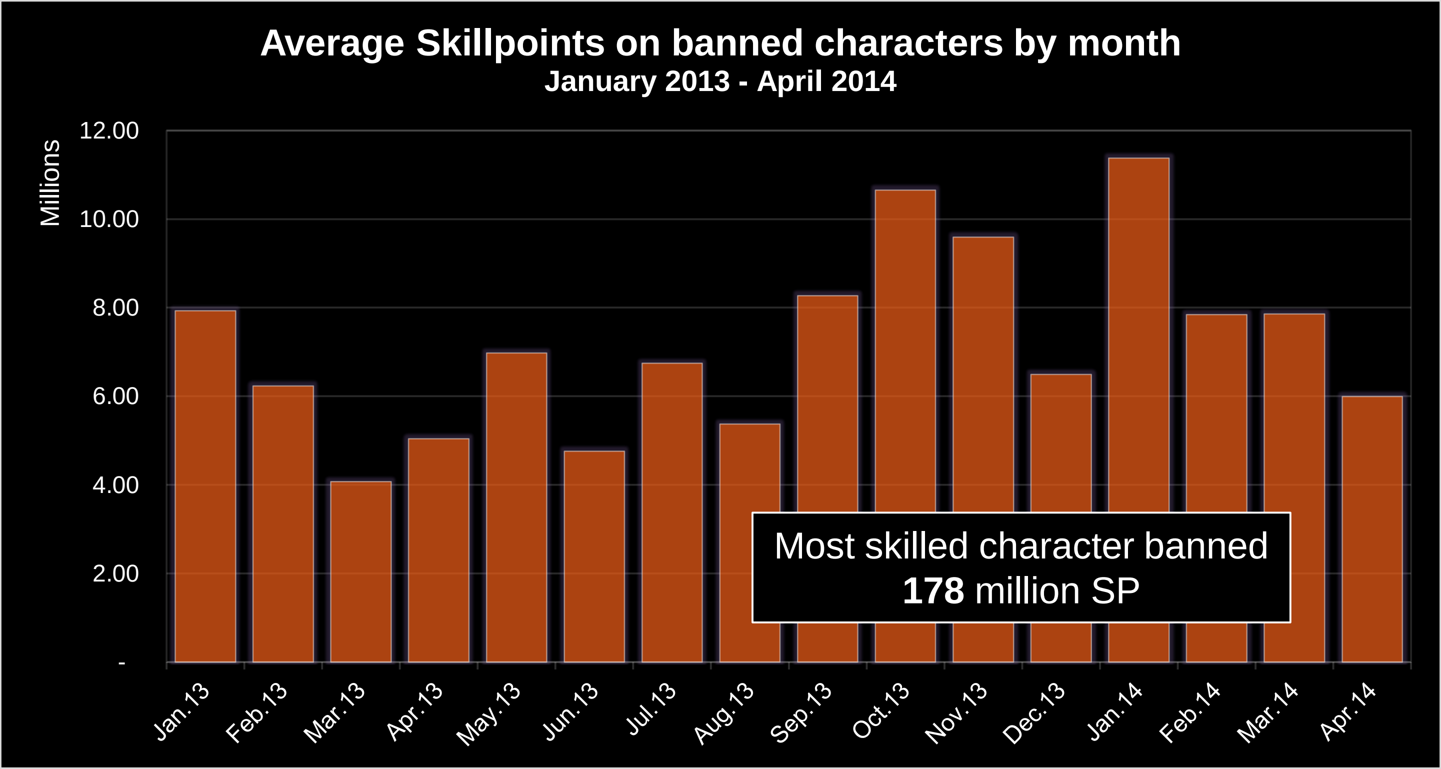
Modified Client	6,019
ISK Selling	5,463
ISK Buying	1,334
Macro Use	17,386
Total:	**30,202**

Banned accounts by country (IP)



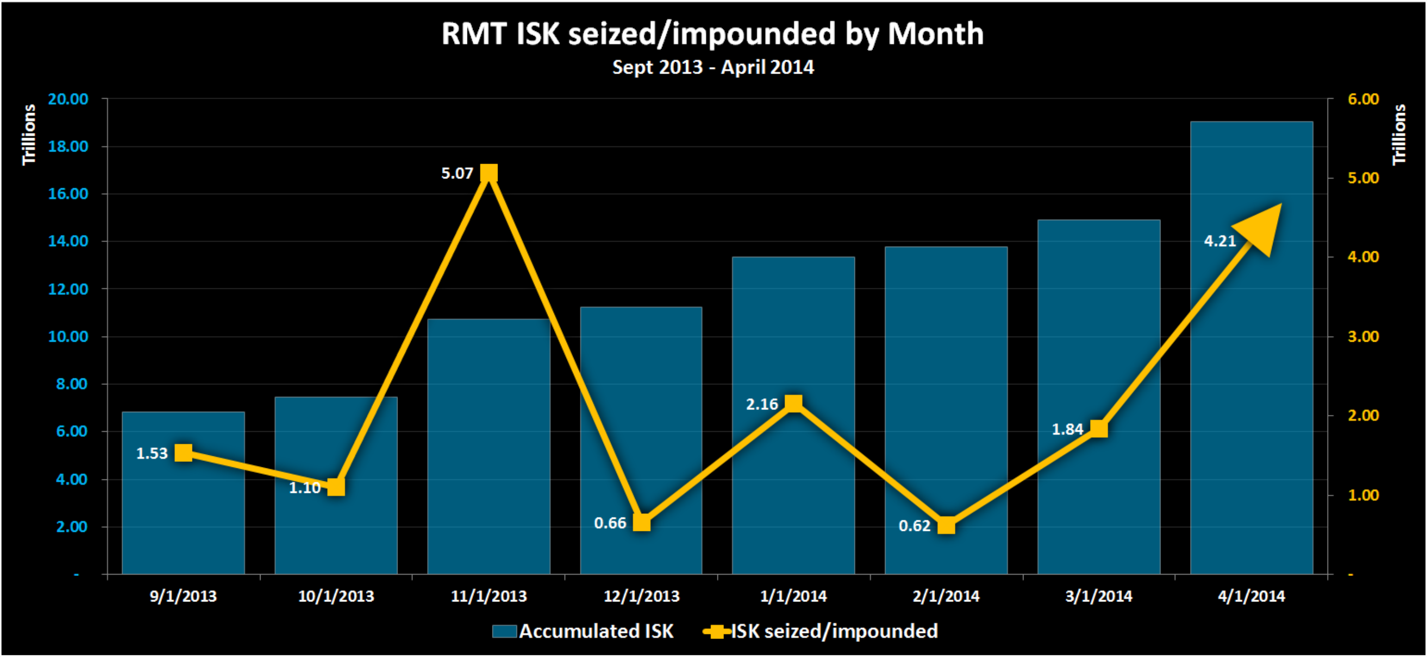
Mucho Skillpoints KAPUTT

EVE FANFEST 2014



Most skilled character banned
178 million SP

Mucho ISK KAPUTT

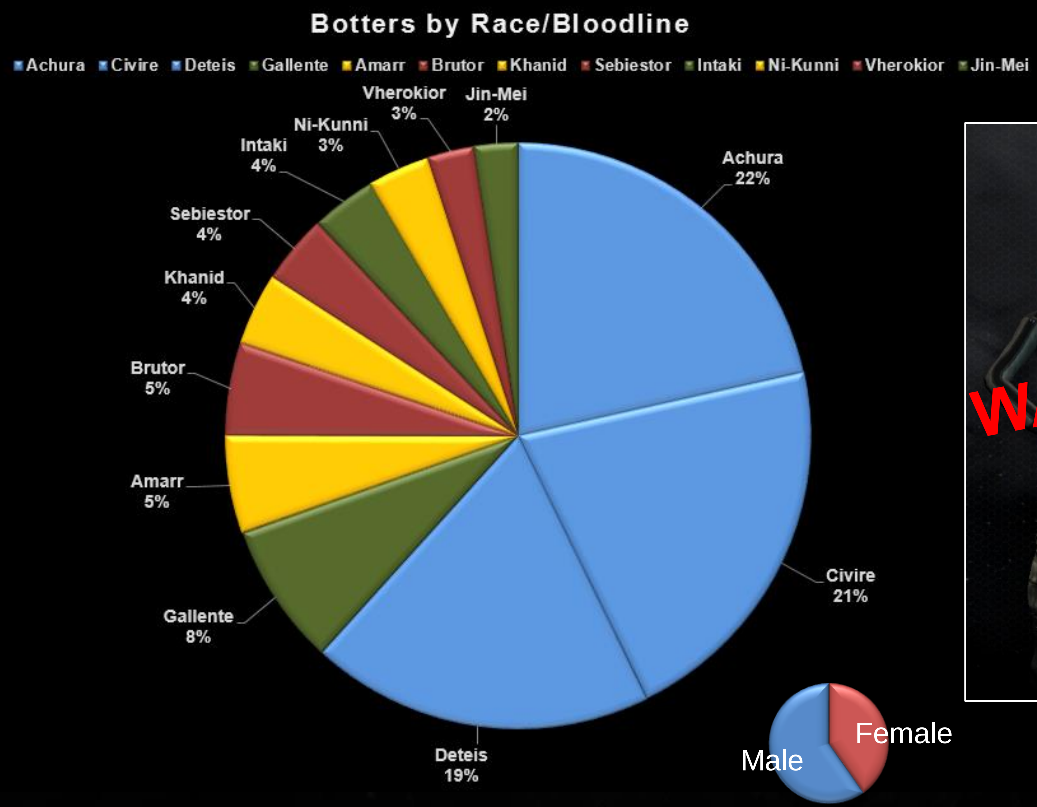


- Just over 16k accounts
- 5.287 ISK Buyers
- 10.936 Bots
- Roughly 750 m/account
- No assets – only raw ISK

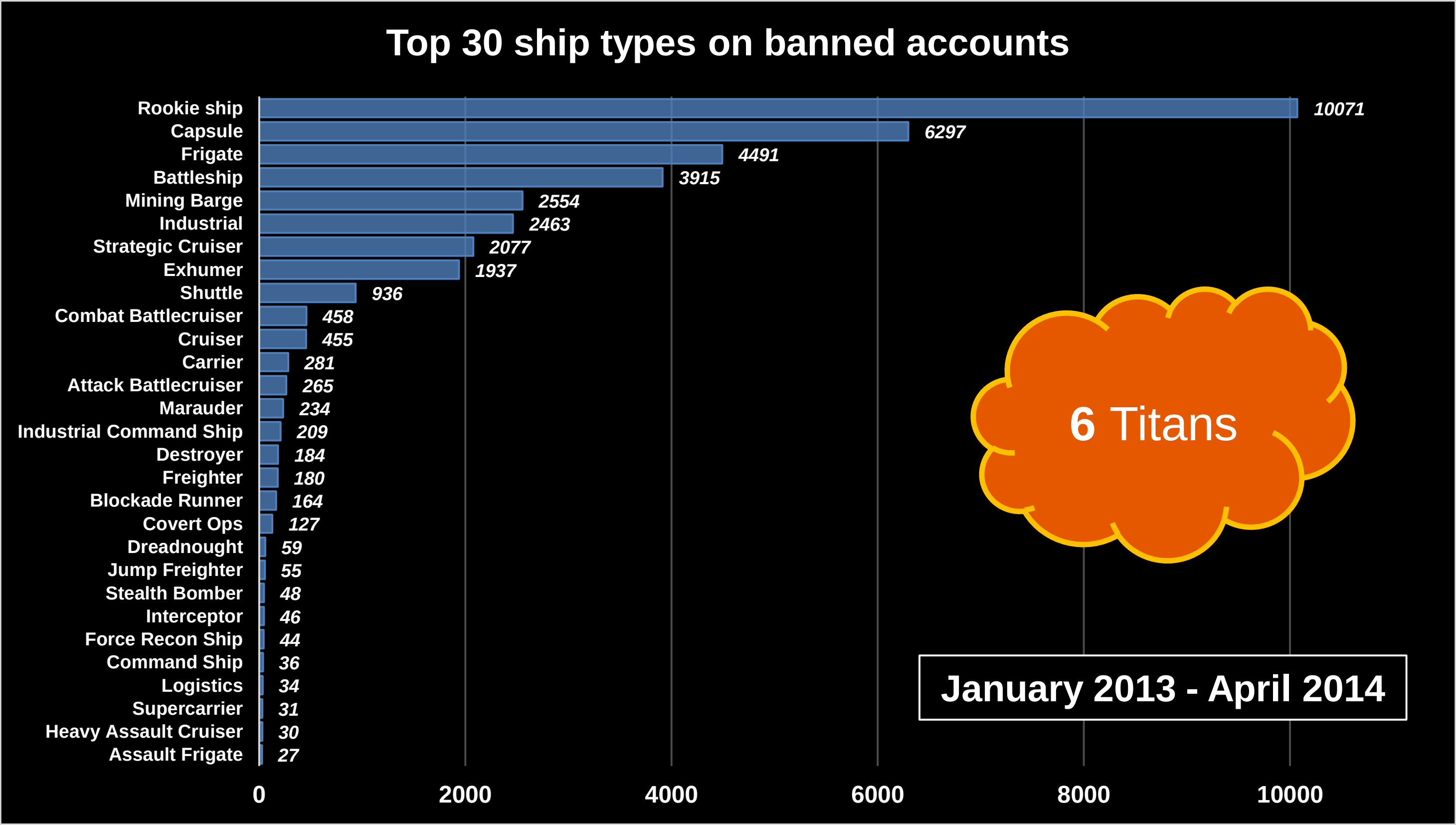
Value of assets coming soon

Banned botters by race/bloodline

January 2013 - April 2014



Ship types on banned accounts

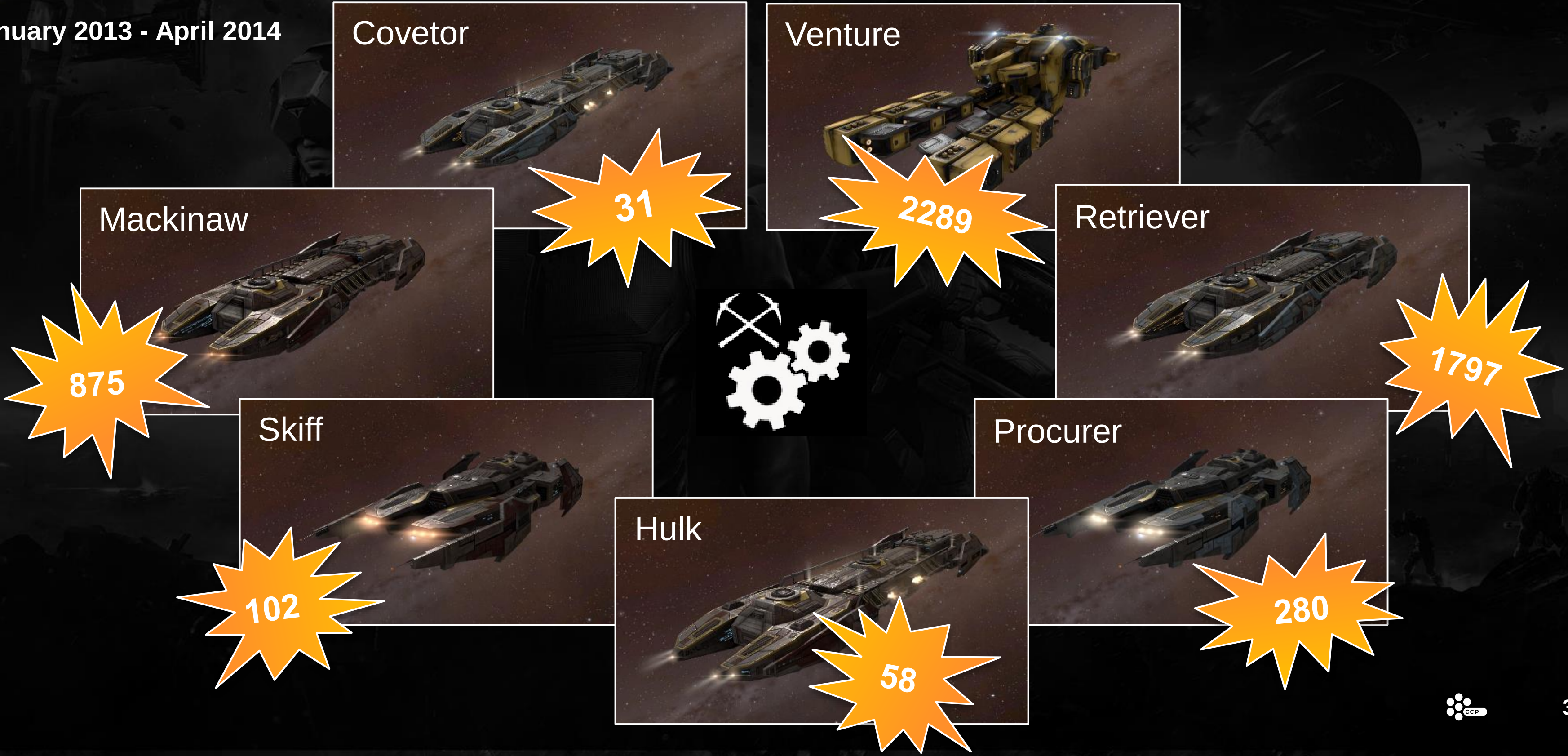


6 Titans

January 2013 - April 2014

Ship types on banned mining bots

January 2013 - April 2014



Covetor 31

Venture 2289

Mackinaw 875

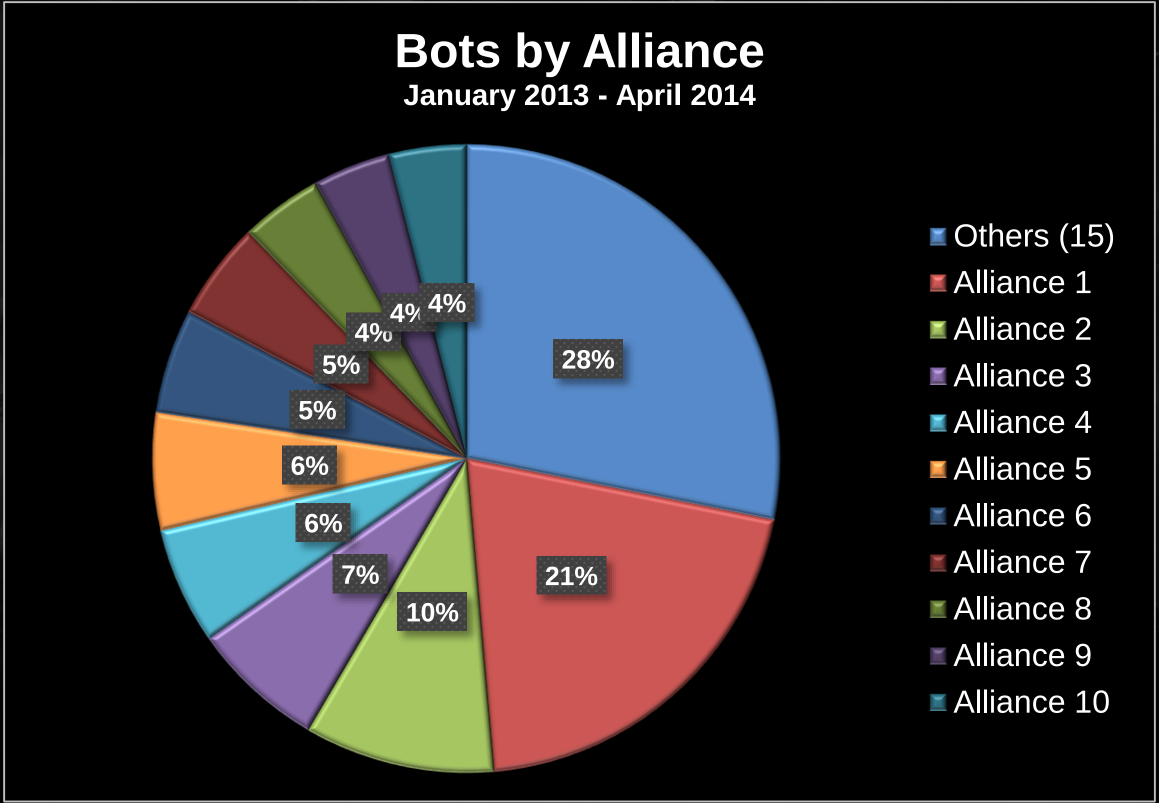
Retriever 1797

Skiff 102

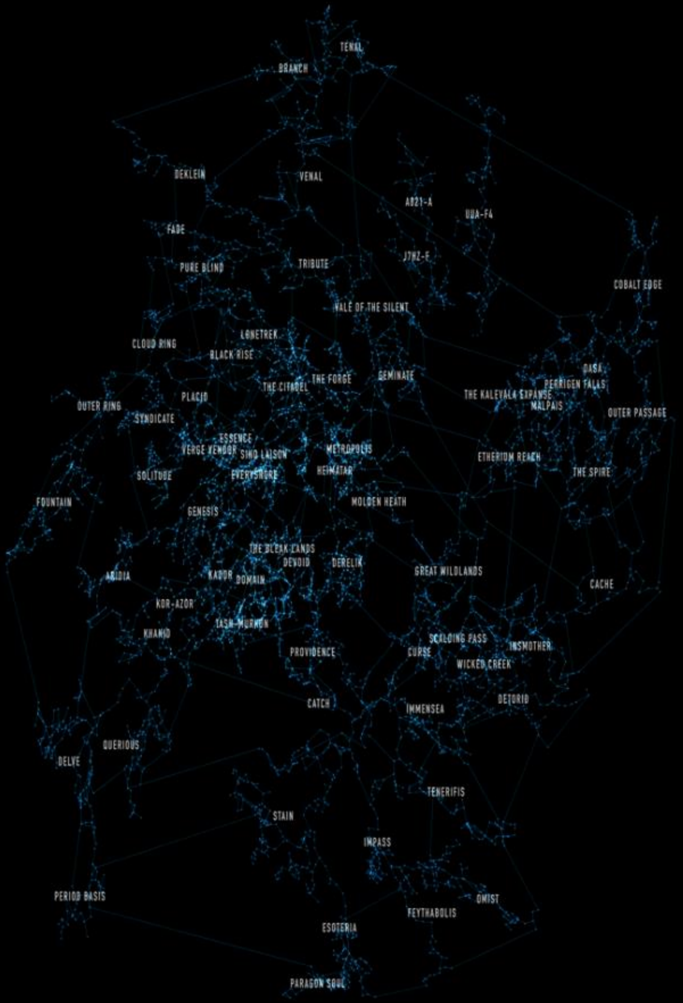
Procurer 280

Hulk 58

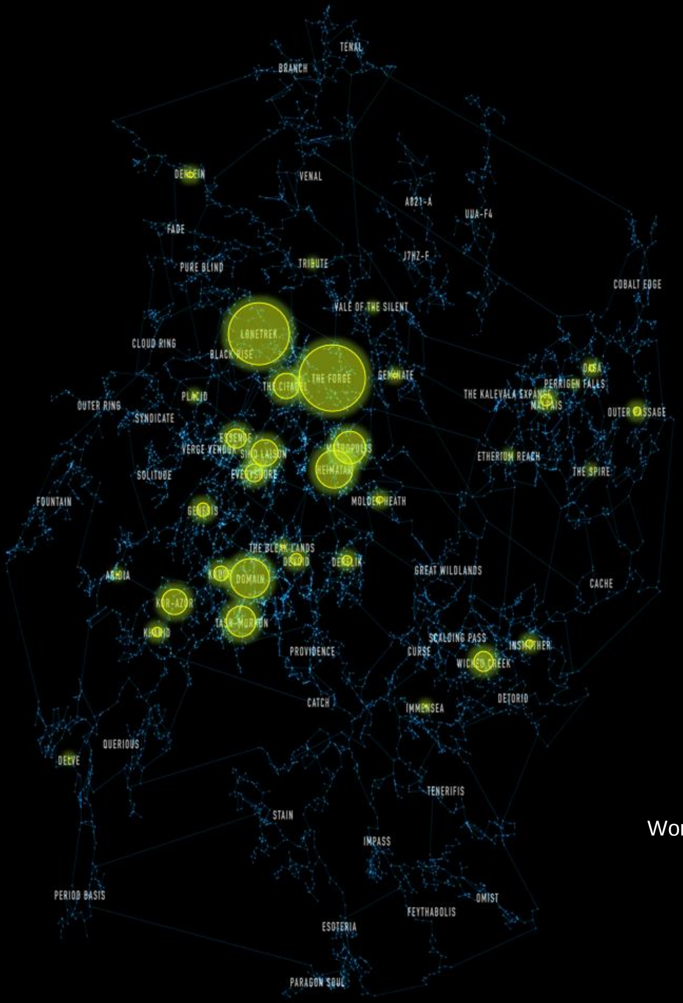
Banned botting accounts by Alliance


Bots by Alliance
January 2013 - April 2014

Lovely **EVE** world map



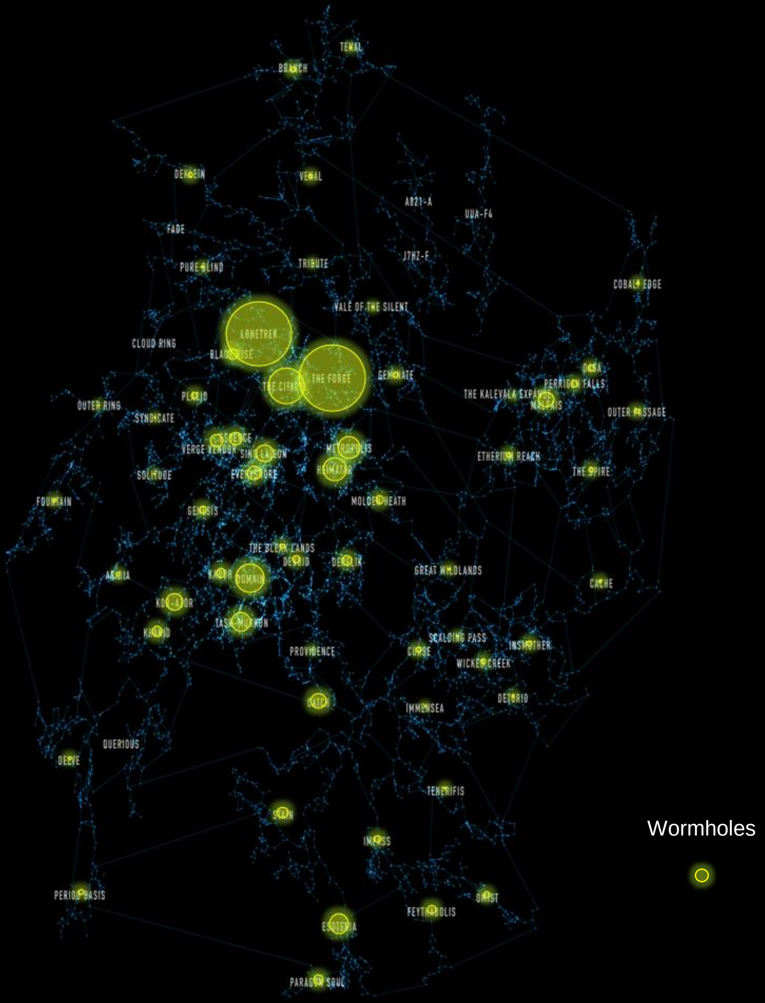
Bots banned by region
Mining bots



Wormholes

January 2013 - April 2014

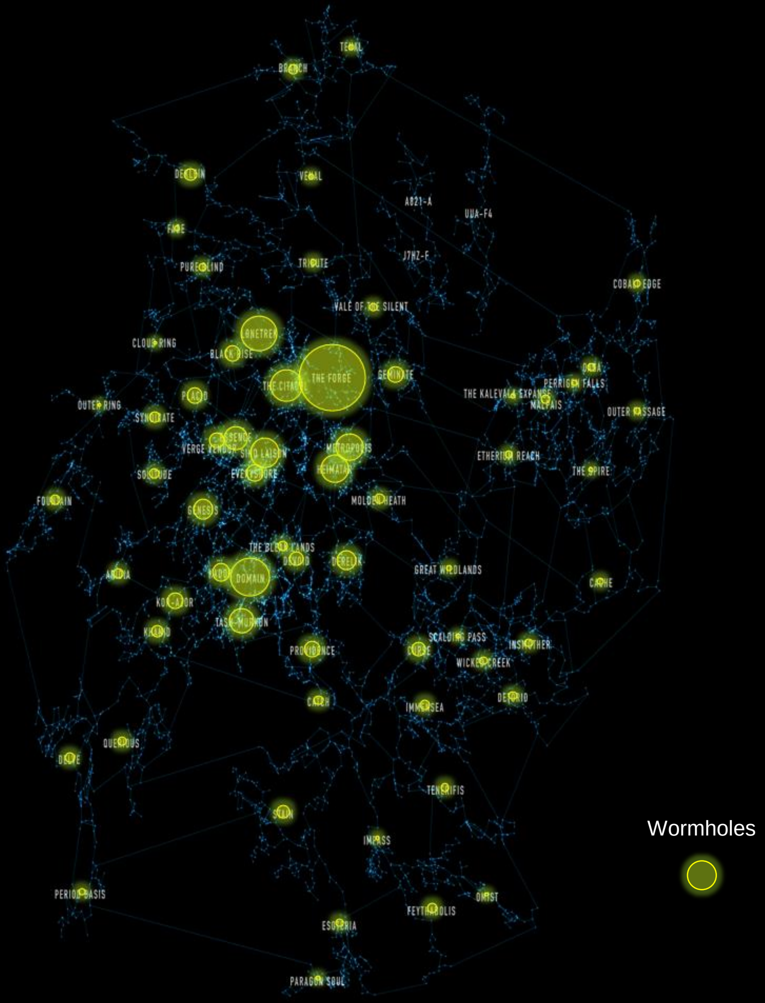
Bots banned by region
Combat bots



January 2013 - April 2014

ISK Buyers by region

$



January 2013 - April 2014

The Post-Ban Stories

- Suffering from insomnia
- Framed by disgruntled spouse
- Sleeping with Laptop in bed for warmth
- Accidentally left head-phones on keyboard
- On Meth
- Little brother did it

Security Tips & Tricks

Sec Tips & Tricks :: Account Security

- Account Sharing
  - Is **not** allowed. You might show up on our radar and we might ban you for it.
  - For us this can look like the account has been hacked
  - Indicators like region changes are taken into account

Sec Tips & Tricks :: Account Security

- Password Security
  - Password security is not only about strong passwords
  - If you reuse your password with another service this puts your game accounts at risk as well
  - We detect and react on excessive brute force attempts

Sec Tips & Tricks :: Account Security

- IP / Region Monitoring
  - We always had the possibility to leverage this information for account security topics
  - Recently we enhanced the automation and we still keep improving it
  - Additional, related, functionality (restricting accounts for access from specific regions / IPs) are being evaluated

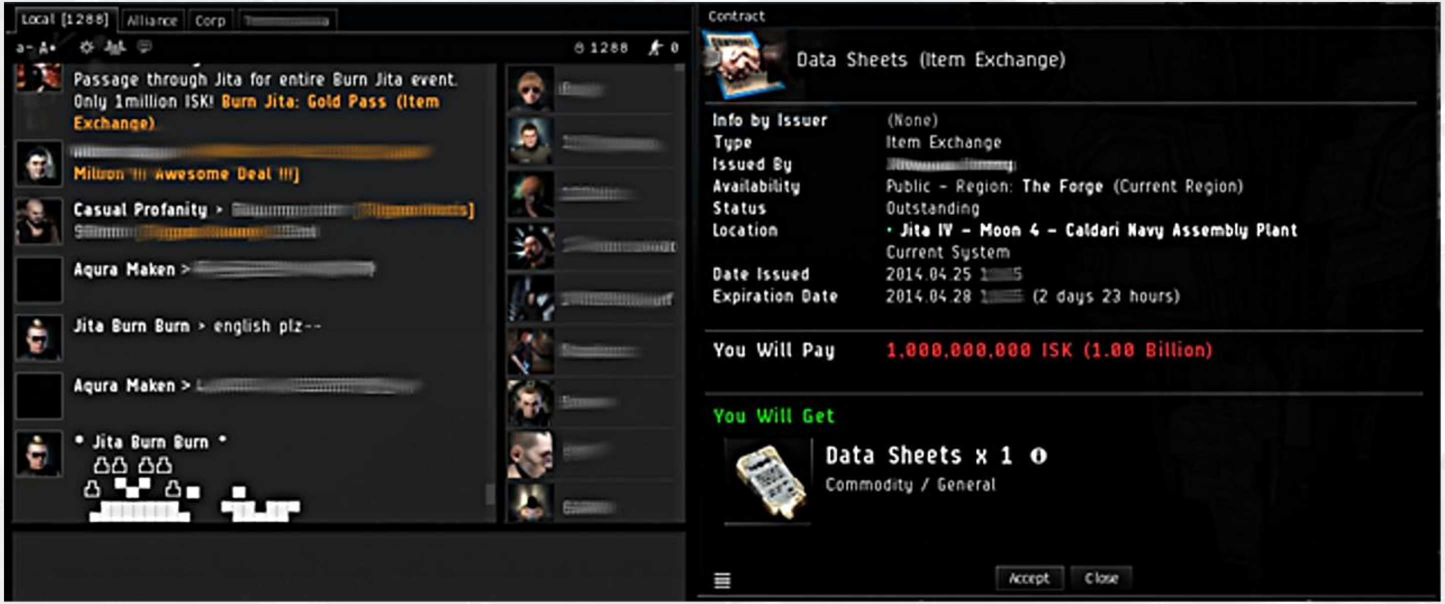
Sec Tips & Tricks :: Account Security

- E-Mail Address Validation
  - We already rely on email as the contact medium to you
  - Since summer 2013 you have to validate your email address with the registration of a new account
  - We encourage you to update the contact information of all your accounts – this is relevant information we need in order to proceed with further security measures

Sec Tips & Tricks :: Account Security

- Future Plans
  - Multi factor authentication has been on the ‘nice to have list’ for years
  - It’s still something we aim for, but we need to get all the prerequisites fixed and in place first
  - A very crucial requirement is a trusted and validated way to stay in contact with you
  - We need at least valid email addresses of all of you! Please take a first step with us and validate your email address at https://secure.eveonline.com !

Sec Tips & Tricks :: Scamming



Passage through Jita for entire Burn Jita event. Only 1million ISK! Burn Jita: Gold Pass (Item Exchange)

[redacted] Milion !!! Awesome Deal !!!]

Casual Profanity > [redacted]

Aqura Maken > [redacted]

Jita Burn Burn > english plz--

Aqura Maken > [redacted]

• Jita Burn Burn •

Contract

Data Sheets (Item Exchange)

Info by Issuer	(None)
Type	Item Exchange
Issued By	[redacted]
Availability	Public - Region: The Forge (Current Region)
Status	Outstanding
Location	• Jita IV - Moon 4 - Caldari Navy Assembly Plant Current System
Date Issued	2014.04.25 [redacted]
Expiration Date	2014.04.28 [redacted] (2 days 23 hours)

You Will Pay 1,000,000,000 ISK (1.00 Billion)

You Will Get

Data Sheets x 1
Commodity / General

- Triple-check items: Is this the item you are looking for?
- Always compare prices: 1 Million ≠ 1 Billion ISK

Sec Tips & Tricks :: Scamming

- Scamming is not forbidden as long is it stays within the given boundaries!

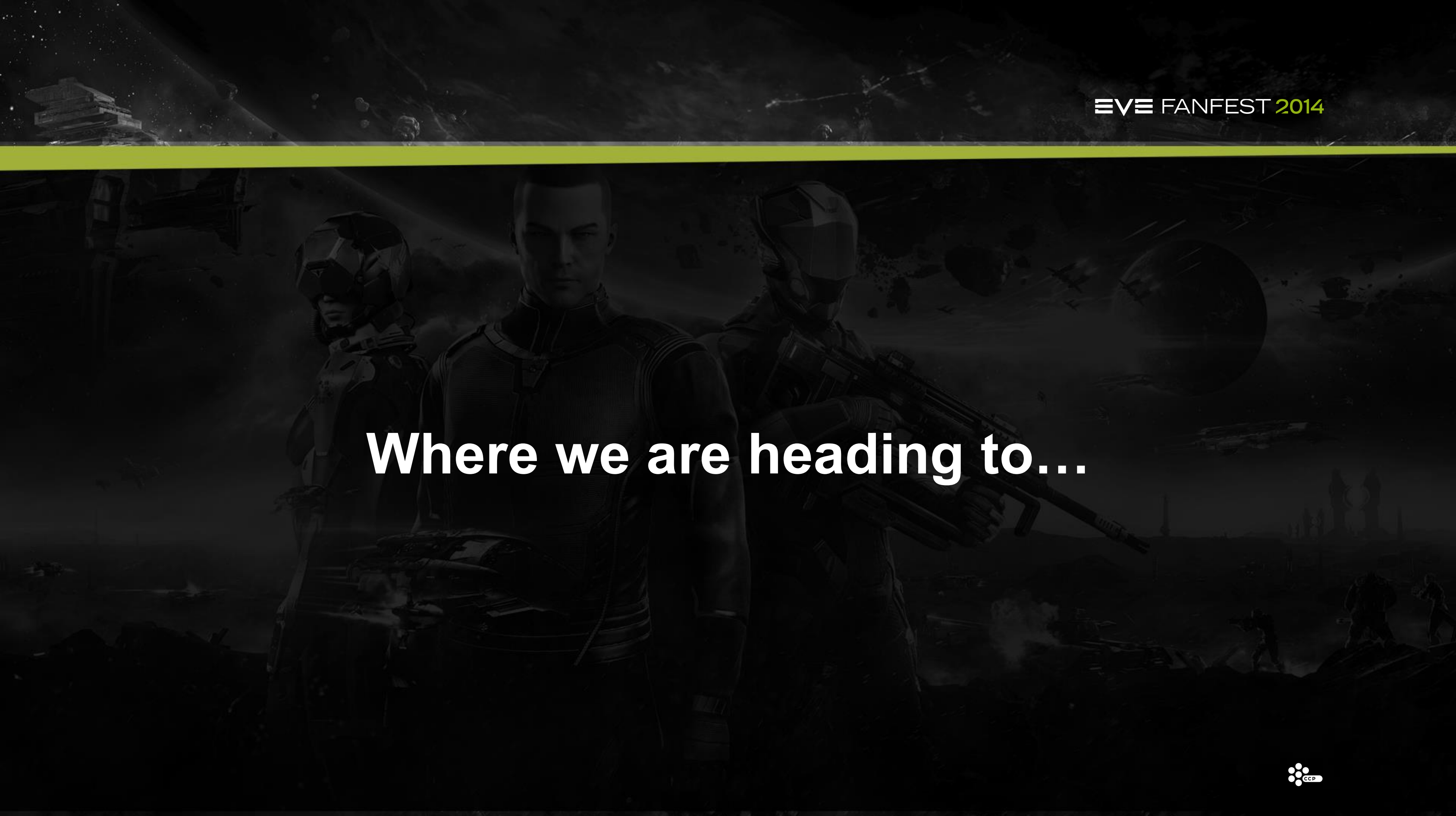
Please make sure to be aware of what is part of EVE Online game play (meta gaming) and check out the Knowledge Base:

http://community.eveonline.com/support/knowledge-base/

Sec Tips & Tricks :: RMT & Fraud

- RMT is not only prohibited, it’s also very dangerous for you
- We will ban you if you are involved
- The RMT organizations will make use of all information you provide them with
- Including
  - Your name and contact information
  - Your billing information (credit card details etc.)
  - Your EVE Accounts

Over 30% of hacked accounts have previously been associated with RMT.



Where we are heading to…

Security Roadmap (Excerpt)

- **Team Security**
  - Enhancing detection and mitigation capabilities as well as increase automation of the process
  - Therefore reducing the time required “*From evidence to bans*”
  - Improve interdepartmental processes
  - Strengthen rules and policy awareness
- **InfoSec**
  - Strengthen the over all security of our infrastructure
  - Improve prevention, detection and remediation capabilities
  - Implement and align security measures and processes globally
- **Both**
  - Account Security
    - Utilization of email verification system for various functionality
    - Improvement of account usage (region and suspicious activity) monitoring
    - Evaluation of additional account security features we can offer as services to **you**, our most important assets! (e.g. region/IP restriction & multi factor)

Stereotypes

- Caldari
- Venture
- Mining in Lonetrek/The Forge
- On Meth
- Little brother

You‘re probably going to look something like this

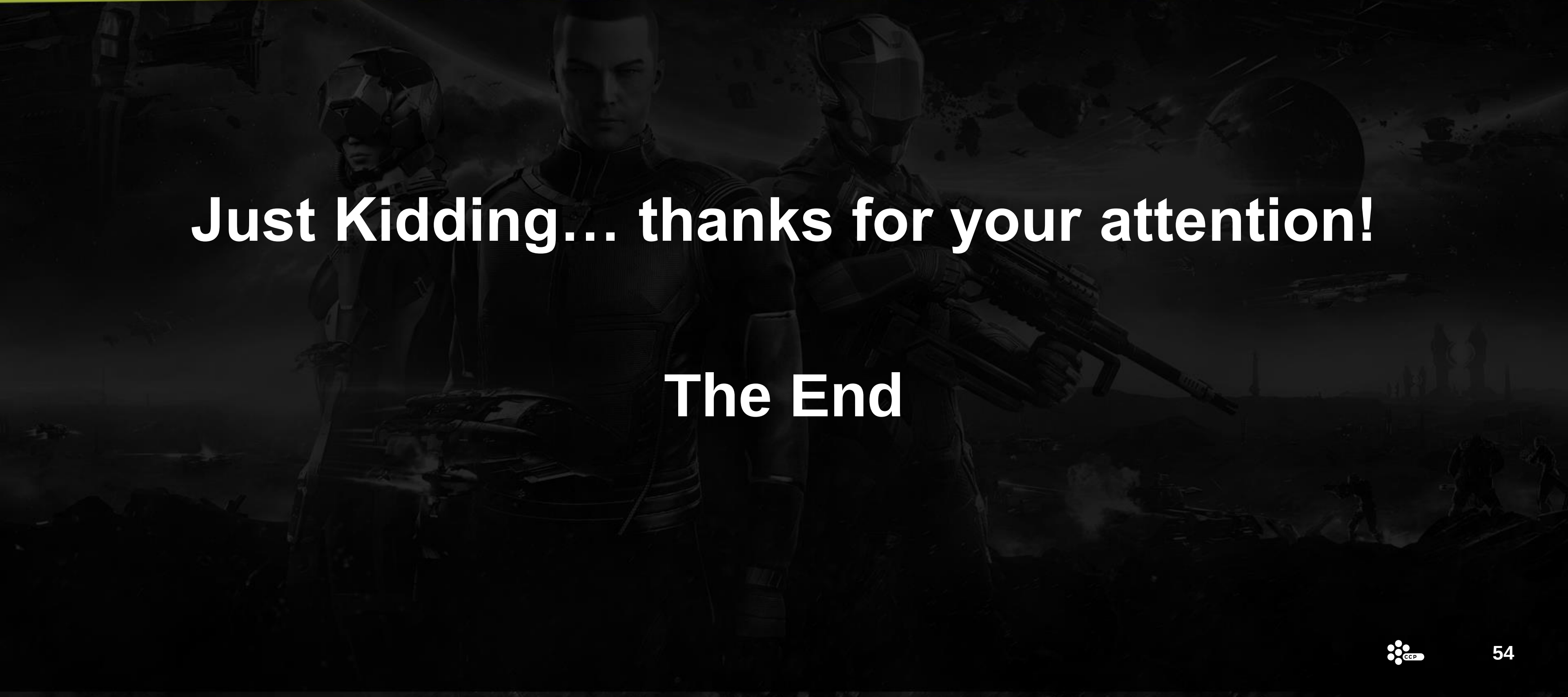
Before botting

After botting

And we‘ll be keeping an eye on you

☺

EULA Proof Reading Session



Just Kidding… thanks for your attention!

The End