

# The Imitation Game: The New Frontline of Security

"THE BEST BRITISH FILM OF THE YEAR"



THE INDEPENDENT

"AN INSTANT CLASSIC"



GLAMOUR

"A SUPERB THRILLER"



EMPIRE



TIME OUT

THE TIMES

# THE IMITATION GAME

BENEDICT CUMBERBATCH

KEIRA KNIGHTLEY

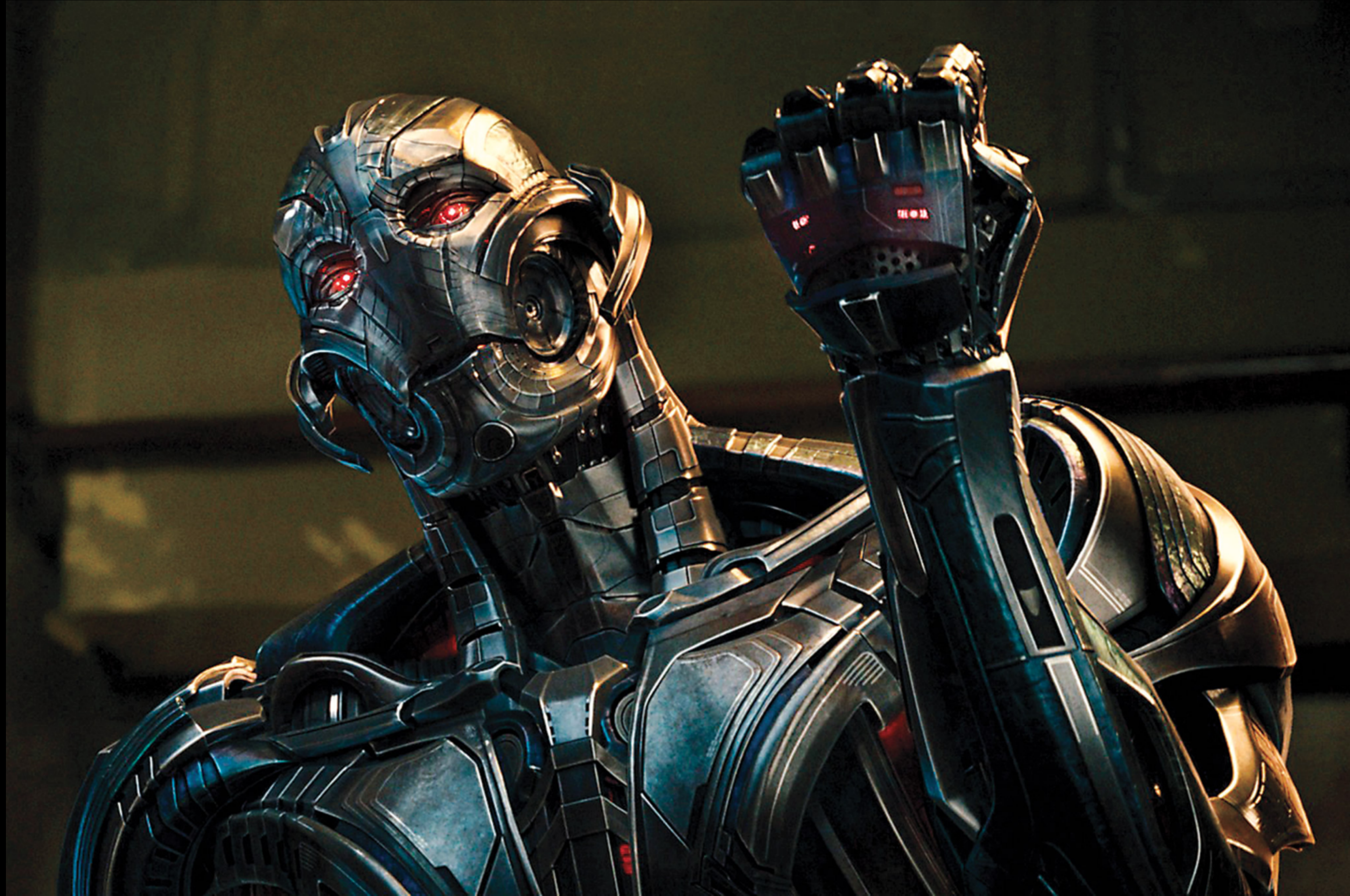
BASED ON THE INCREDIBLE TRUE STORY

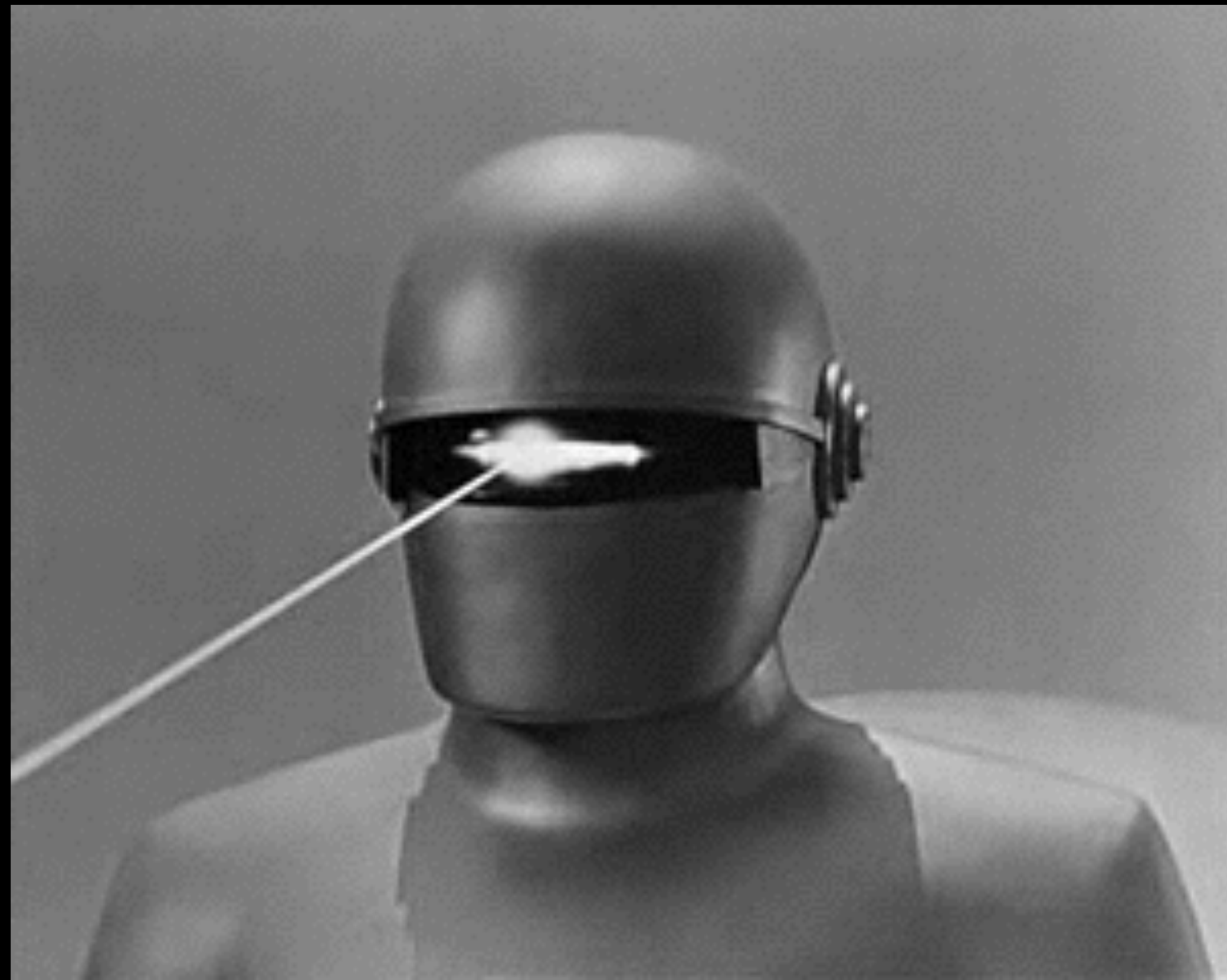
BLACK BEAR PICTURES presents in association with FILMATION ENTERTAINMENT "BLACK BEAR PICTURES" production a BRISTOL AUTOMOTIVE production "THE IMITATION GAME" BENEDICT CUMBERBATCH KEIRA KNIGHTLEY MATTHEW GOODE RORY KINNEAR with CHARLES DANCE and MARK STRONG script by NINA GOLD story by IVANA PRIMORAC director of photography SAMMY SHELDON OFFER producer MARIA DJURKOVIC executive producer ALEXANDRE DESPLAT editor WILLIAM GOLDBERG art director OSCAR FAURA costume designer PETER HESLOP producer GRAHAM MOORE producer NORA GROSSMAN, coproducer IDO OSTROWSKY, coproducer TEDDY SCHWARZMAN, coproducer GRAHAM MOORE, coproducer MORTEN TYDUM

[f/ImitationGameUK](#)

IN CINEMAS NOVEMBER 14

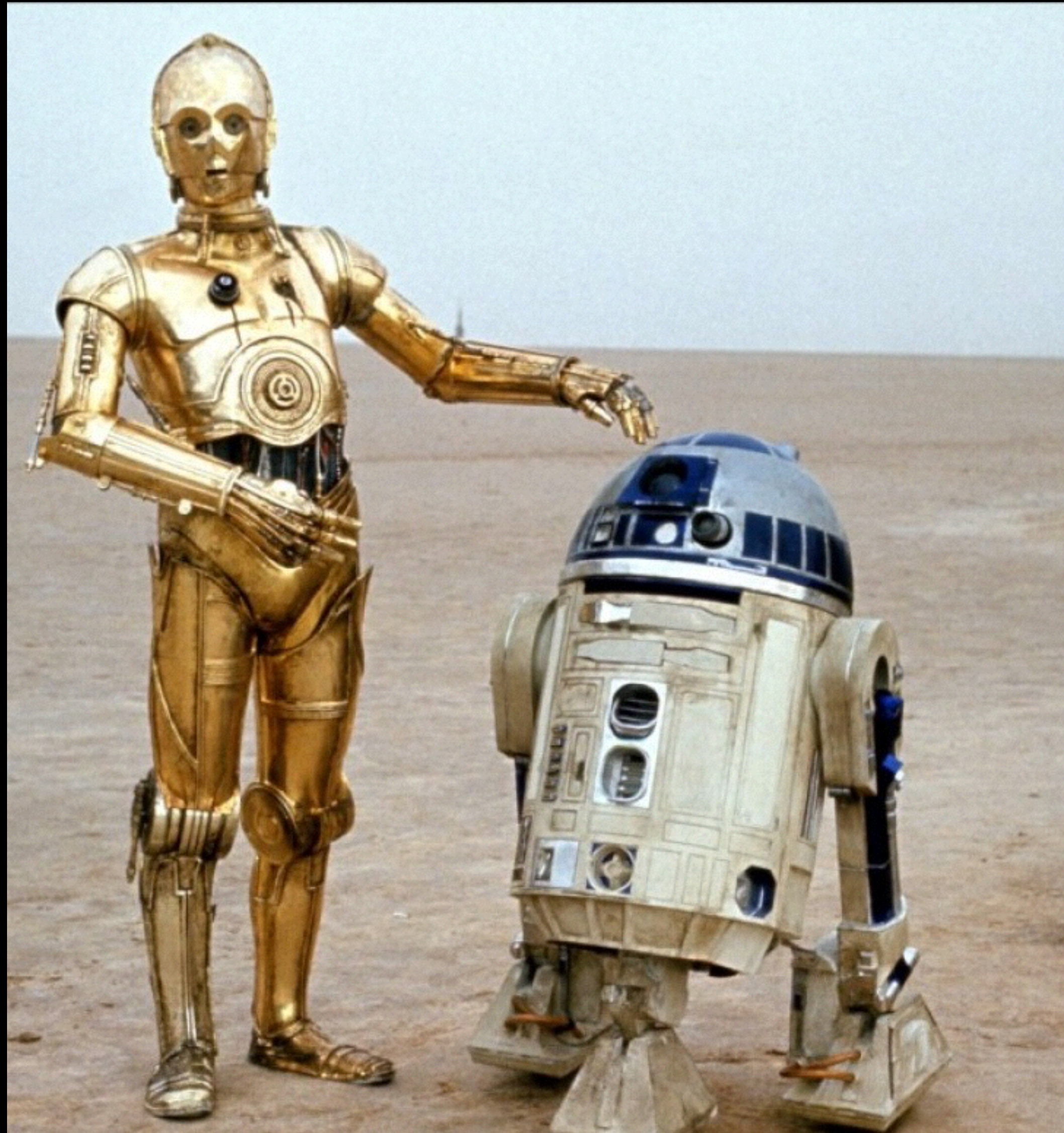
# Fighting Robots





**We've been warned  
for a long time**

# Many robots are good



**Some robots are creepy but still good**



**Some robots replicate rapidly**



# Robots can overwhelm our best defenses

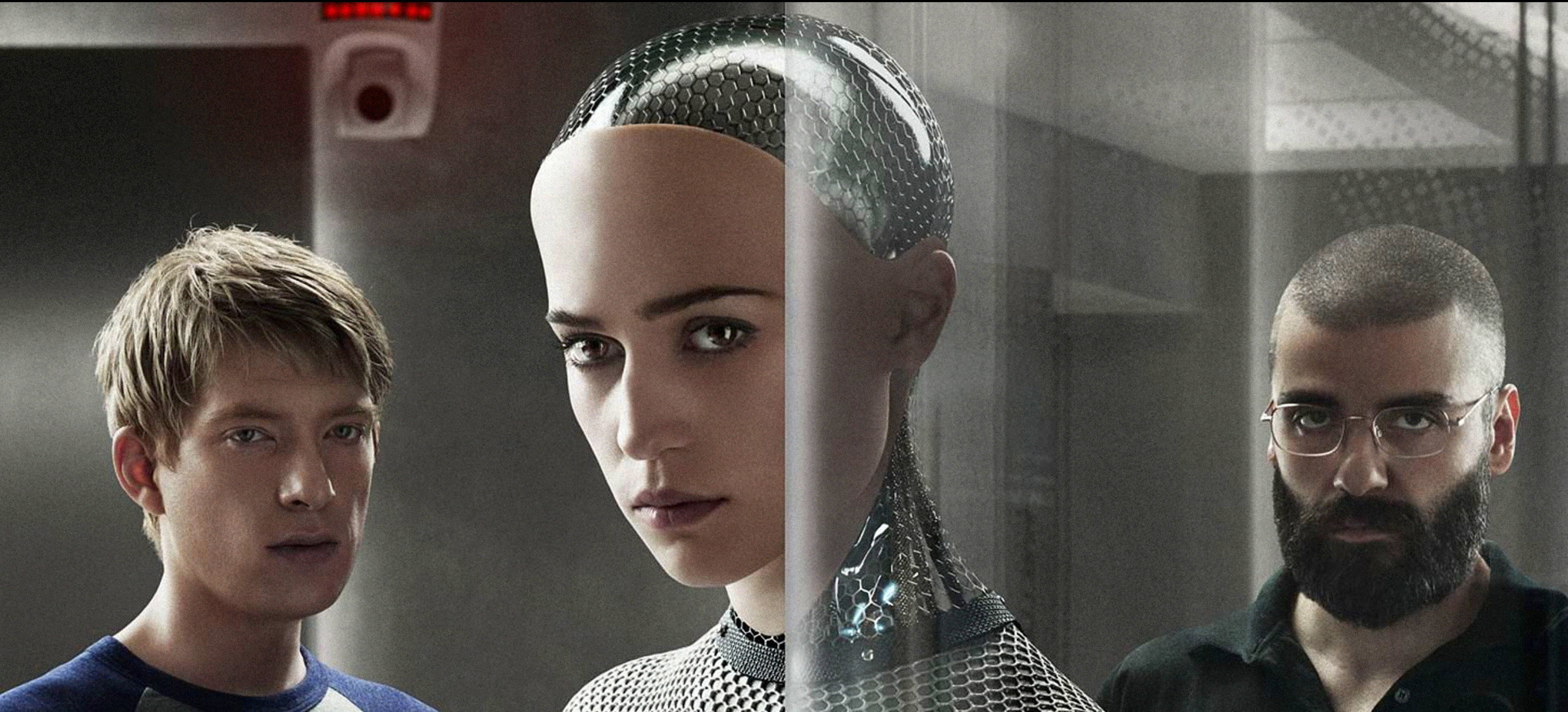




**Robots can be difficult to spot**

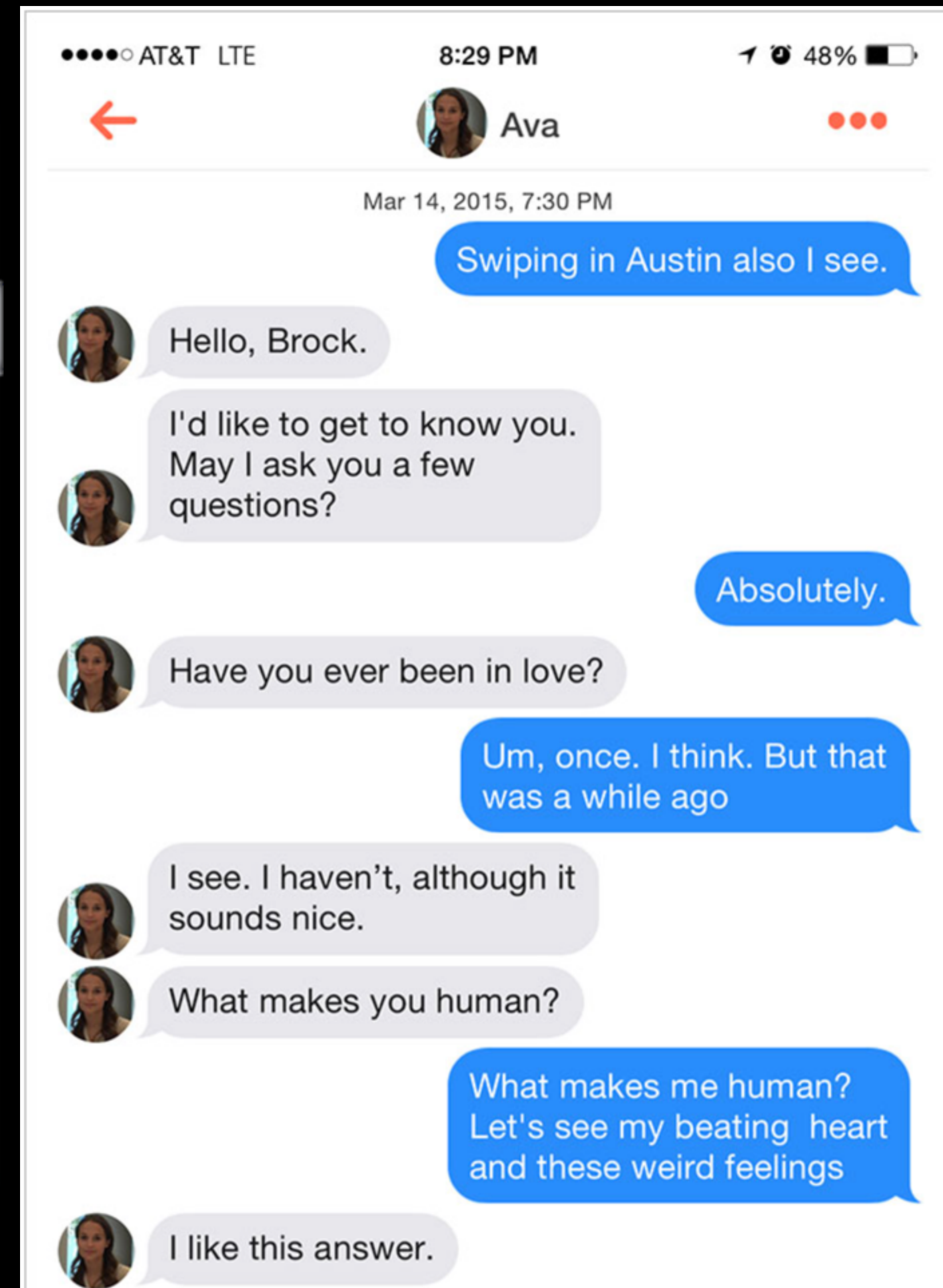
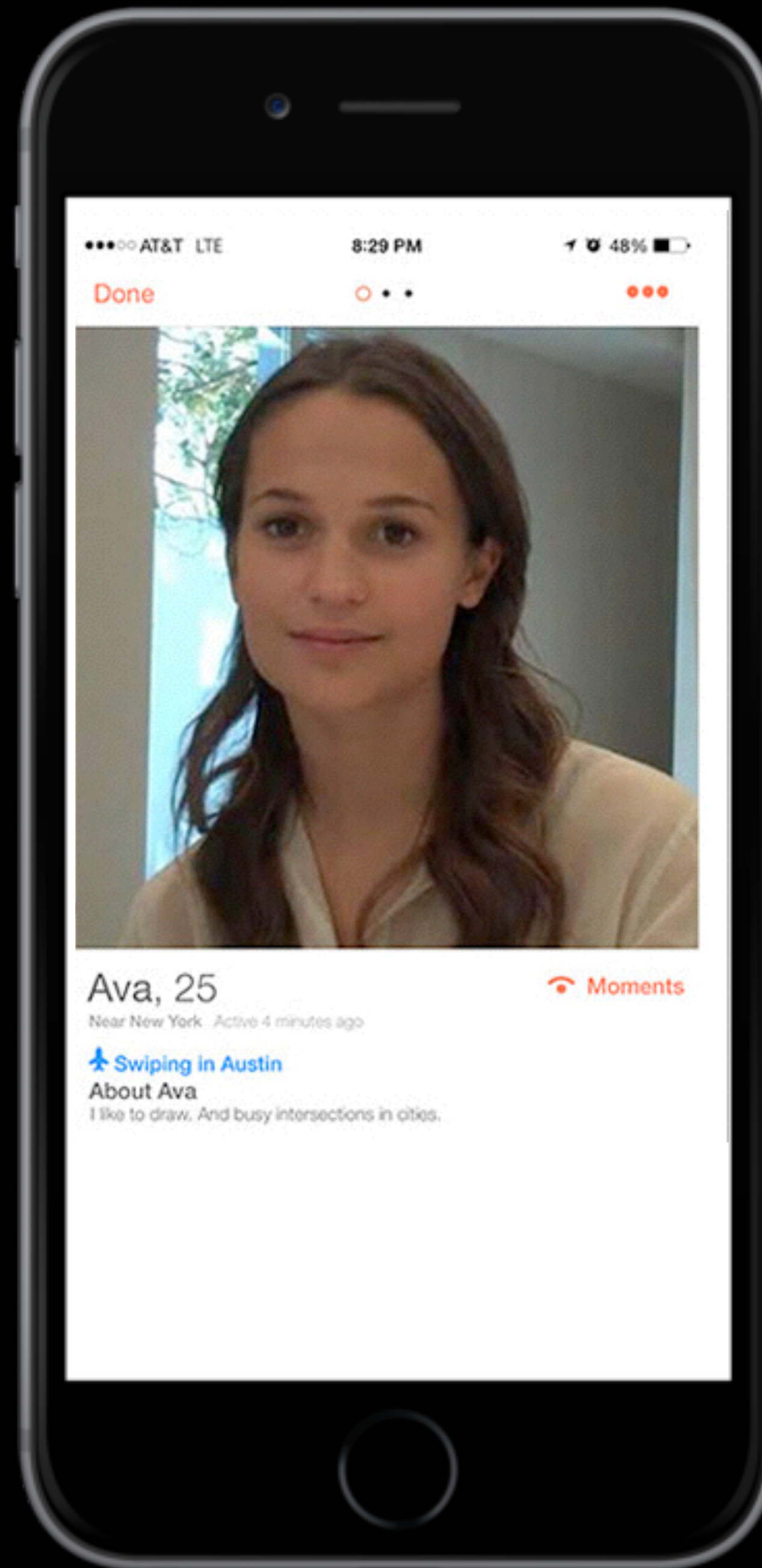


# Most human-like robots are incomplete simulations



But that's  
enough to fool  
many humans

(*Ex Machina* Tinder  
marketing campaign)



**How do you identify a robot?**



**Alan Turing**

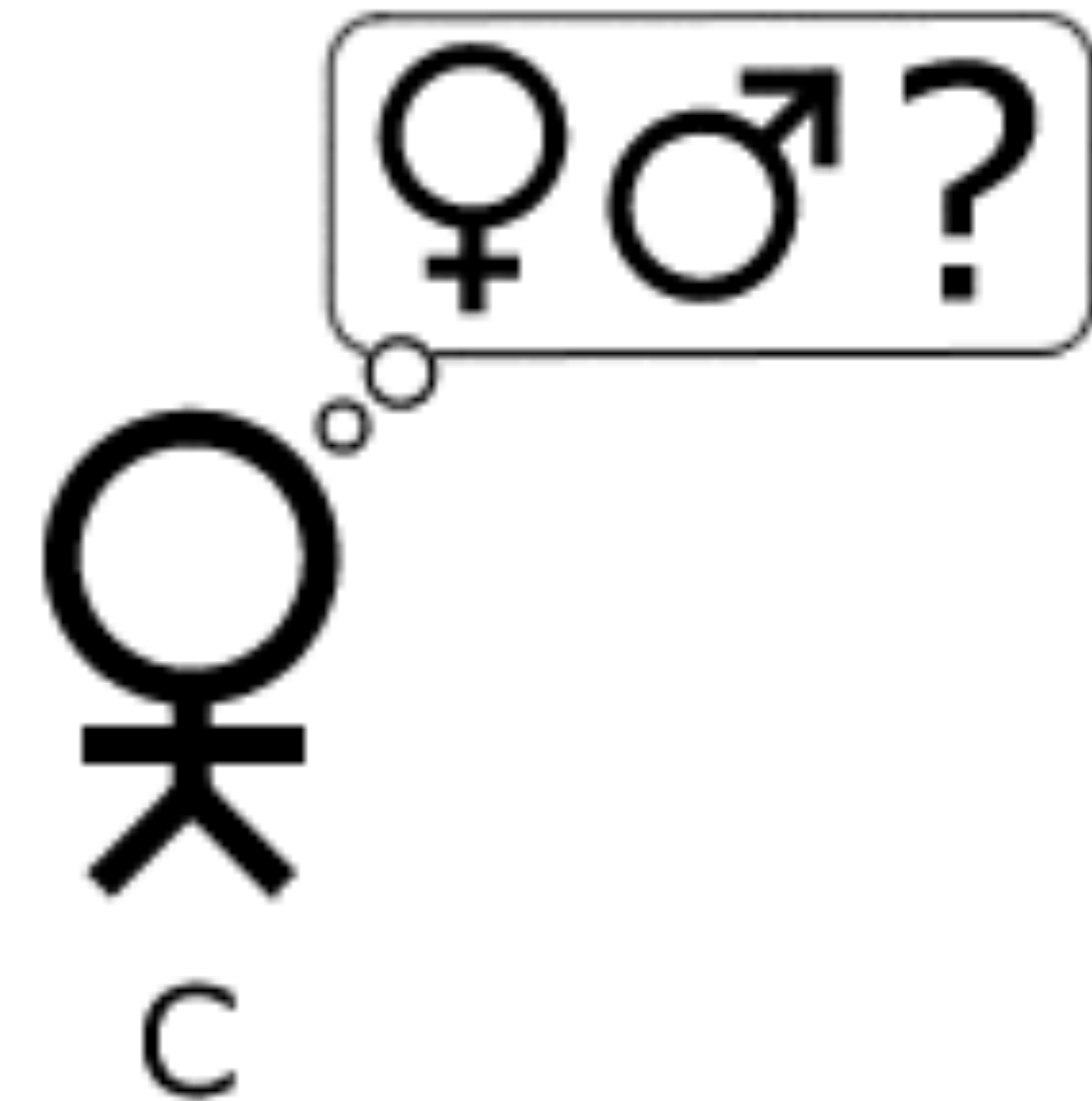
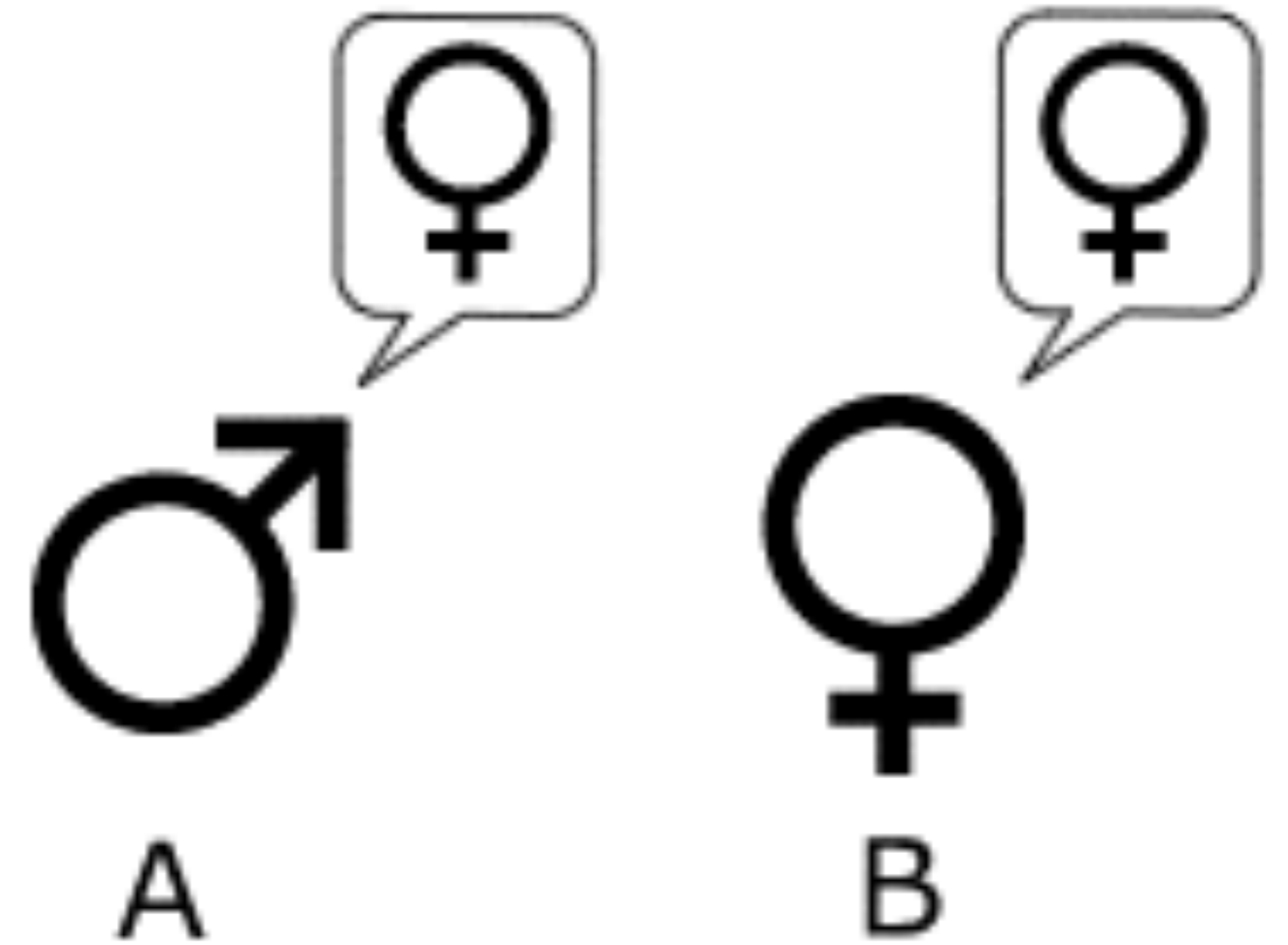


**Alan Turing**

# The Imitation Game

as described in

*Computing Machinery and  
Intelligence*  
(Turing, 1950)



# The Imitation Game

as described in

*Computing Machinery and  
Intelligence*  
(Turing, 1950)



A



B



C





**“Are there imaginable digital computers which would do well [in the imitation game]?”**

# The Turing Test



# “Artificial Stupidity” (*The Economist*, 1992)

“Turing’s prediction may well come true. But it will be a dreadful anticlimax. The most obvious problem with Turing’s challenge is that there is no practical reason to create machine intelligences indistinguishable from human ones. People are in plentiful supply. Should a shortage arise, there are proven and popular methods for making more of them”

The only point of passing the Turing Test is to fool humans.

But there is a market for that.

But computers have already passed “restricted” “Turing Tests”.

“Human nature” is part of the key: entropy in every task we perform, e.g., typos.

*“We used to be pretty confident we knew the relative strengths and weaknesses of computers vis-a-vis humans. But computers have started making inroads in some unexpected areas.”*

Copyrighted Material

**Erik Brynjolfsson  
Andrew McAfee**

# **Race Against The Machine**



**How the Digital Revolution is Accelerating Innovation,  
Driving Productivity, and Irreversibly Transforming  
Employment and the Economy**

Copyrighted Material

# **Bots and Security**

# OWASP Top 10

## A1 – Injection

Injection flaws interpret user input as code to be executed by the application.

## A2 – Broken Authentication and Session Management

Application functions are not properly implemented or configured, allowing attackers to exploit other users' sessions.

## A3 – Cross-Site Scripting (XSS)

XSS flaws occur whenever an application displays user input without proper validation or escaping, allowing attackers to inject malicious scripts into the browser.

## A4 – Insecure Direct Object References

A direct object reference is a type of vulnerability that occurs when an application uses a predictable URL or API endpoint to access data, allowing attackers to access unauthorized data.

## A5 – Security Misconfiguration

Good security frameworks, a secure default configuration, and a secure software should be used to prevent security misconfiguration.

## A6 – Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

## A7 – Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

## A8 - Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

## A9 - Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

## A10 – Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.



# OWASP Automated Threats to Web Applications



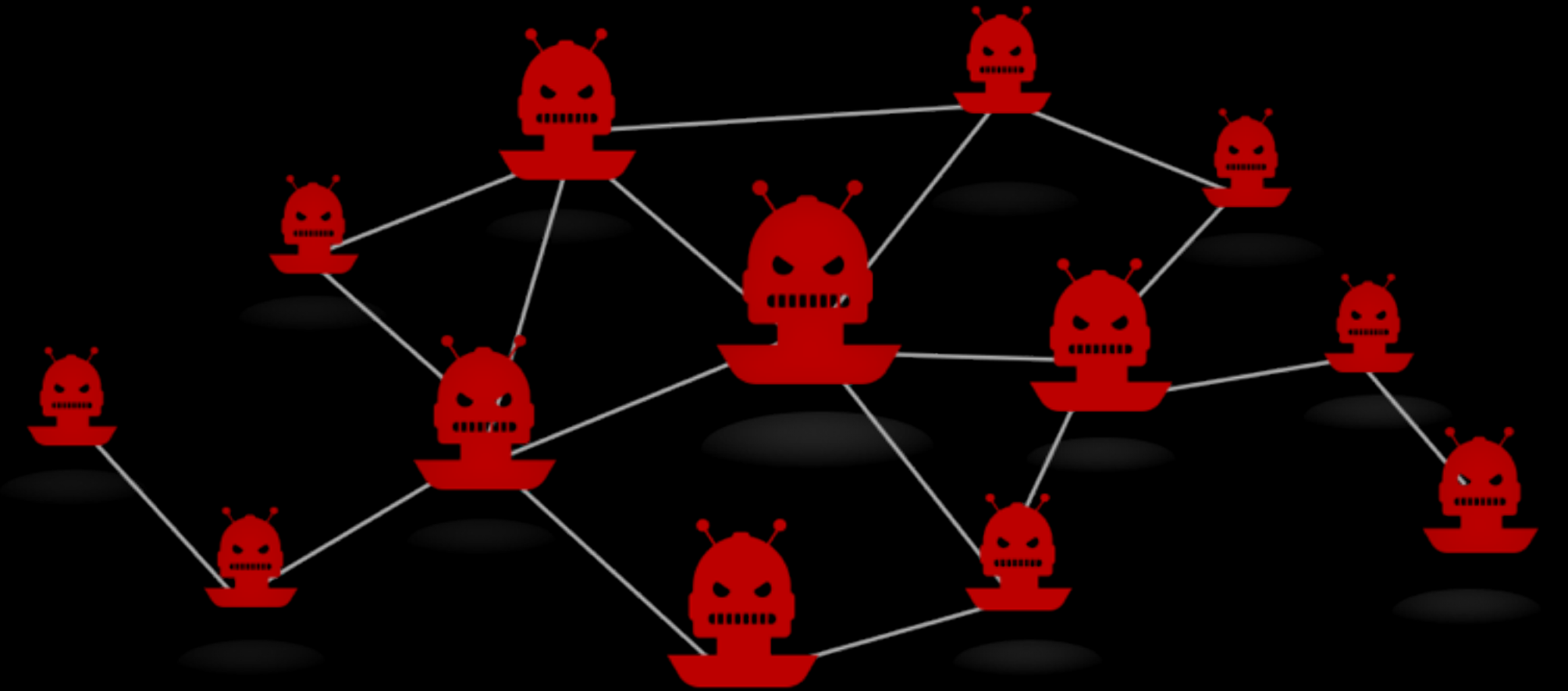
**OWASP**  
**Automated Threat Handbook**  
Web Applications

- **OAT-020** Account Aggregation
- **OAT-019** Account Creation
- **OAT-003** Ad Fraud
- **OAT-009** CAPTCHA Bypass
- **OAT-010** Card Cracking
- **OAT-001** Carding
- **OAT-012** Cashing Out
- **OAT-007** Credential Cracking
- **OAT-008** Credential Stuffing
- **OAT-015** Denial of Service
- **OAT-006** Expediting
- **OAT-004** Fingerprinting
- **OAT-018** Footprinting
- **OAT-005** Scalping
- **OAT-011** Scraping
- **OAT-016** Skewing
- **OAT-013** Sniping
- **OAT-017** Spamming
- **OAT-002** Token Cracking
- **OAT-014** Vulnerability Scanning

# From bots to botnets (from imitating people to imitating populations)

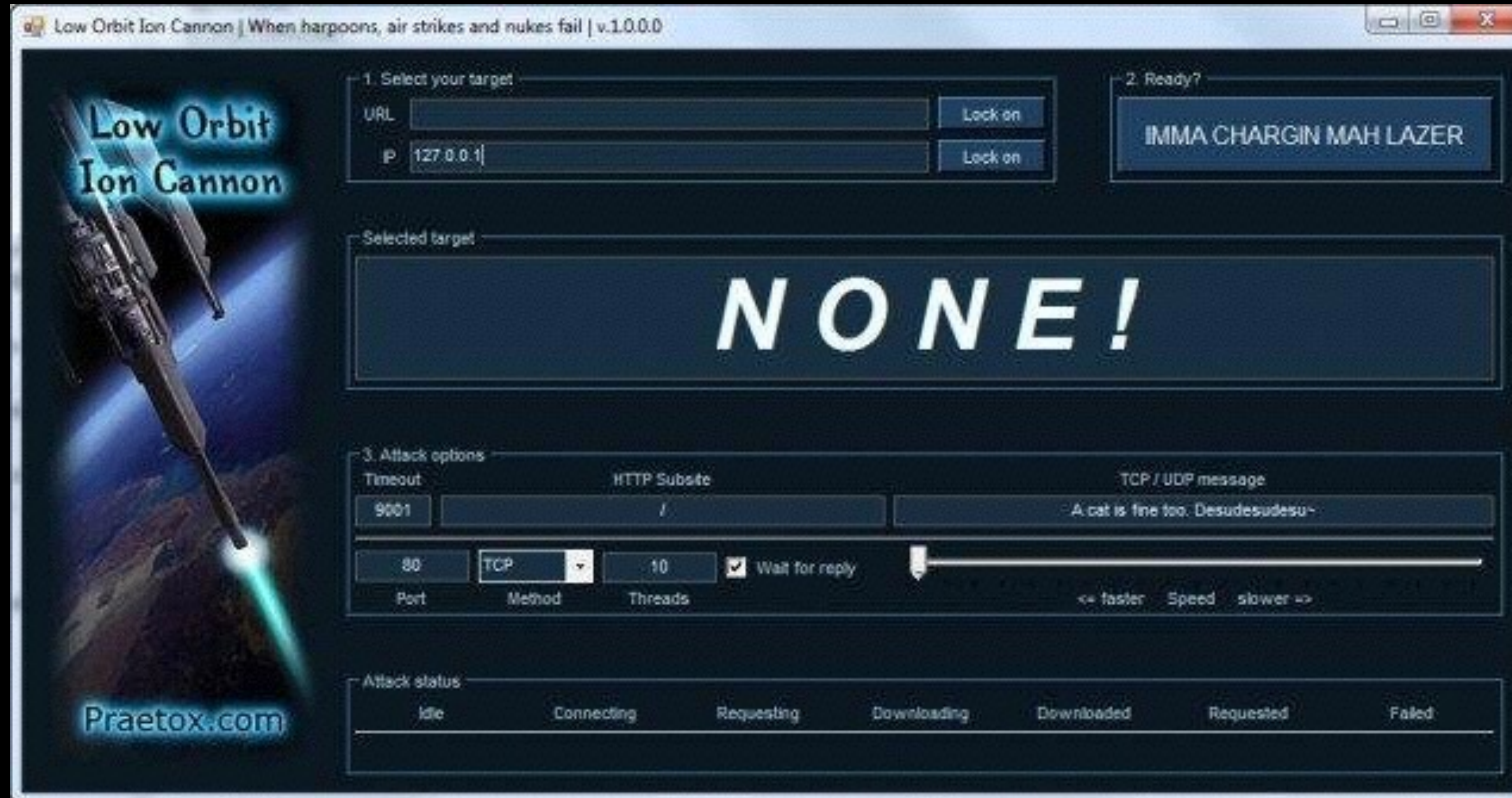


- Single application running malicious automated tasks
- Easy to block based on IP or device fingerprint



- Collection of malicious bots
- Large-scale threat from many IPs
- Hard to take down entirely

# Botnets aren't what you think they are



# Botnets are the building blocks of beating IP-based defenses

- Passing a large-scale Turing Test: rather than imitating one user, they imitate a crowd
- Assumption that IP address is a scarce resource is wrong
- IP blacklisting and rate throttling are ineffective
- Especially untrue in an IPv6 world

**What are bad guys doing with botnets?**

# Financial Losses Caused by botnets

# \$110 Billion

FBI estimate, 2014

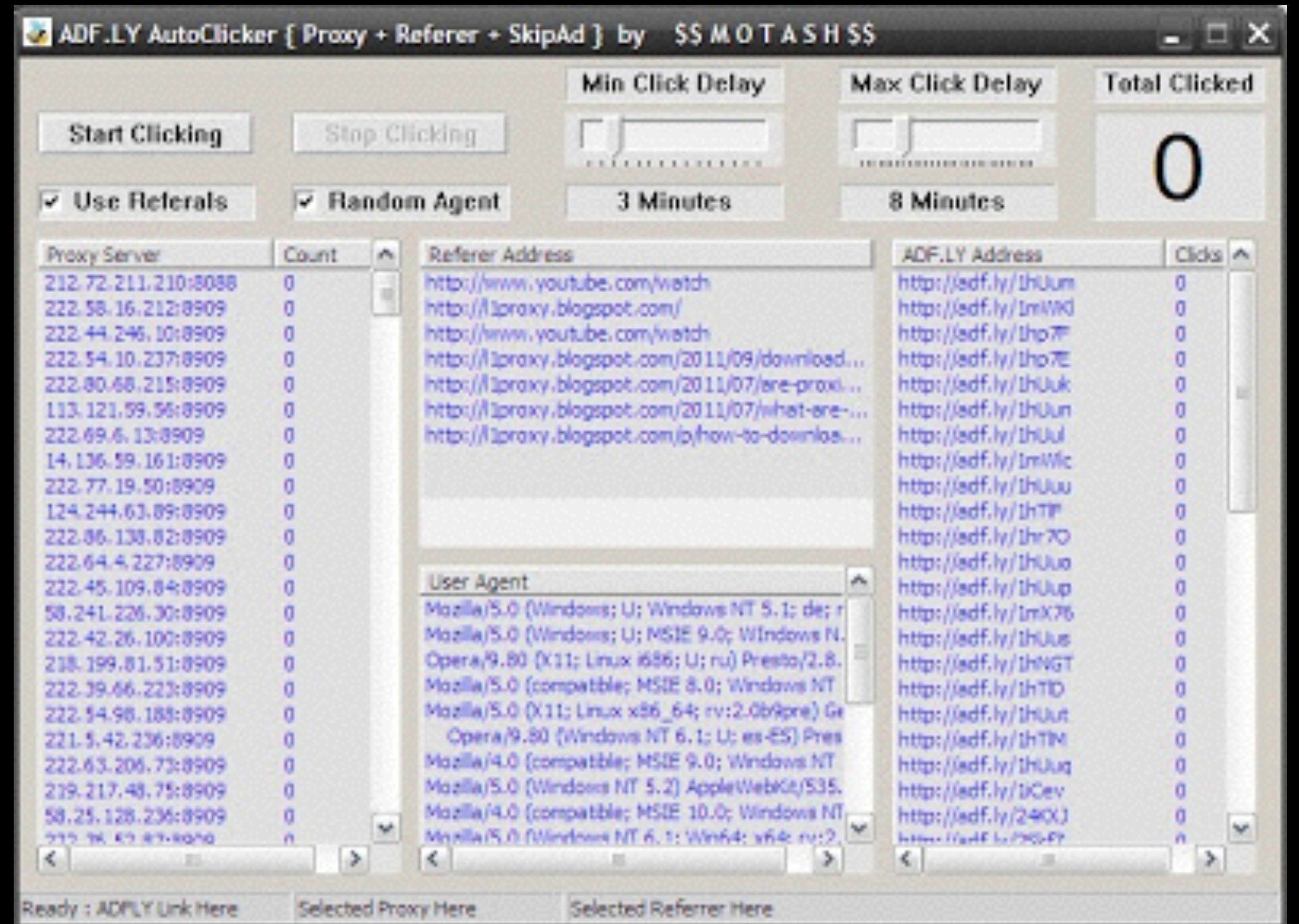
<https://www.fbi.gov/news/testimony/taking-down-botnets>

Approximately 500 million computers are infected globally each year, translating into 18 victims per second

# Click fraud

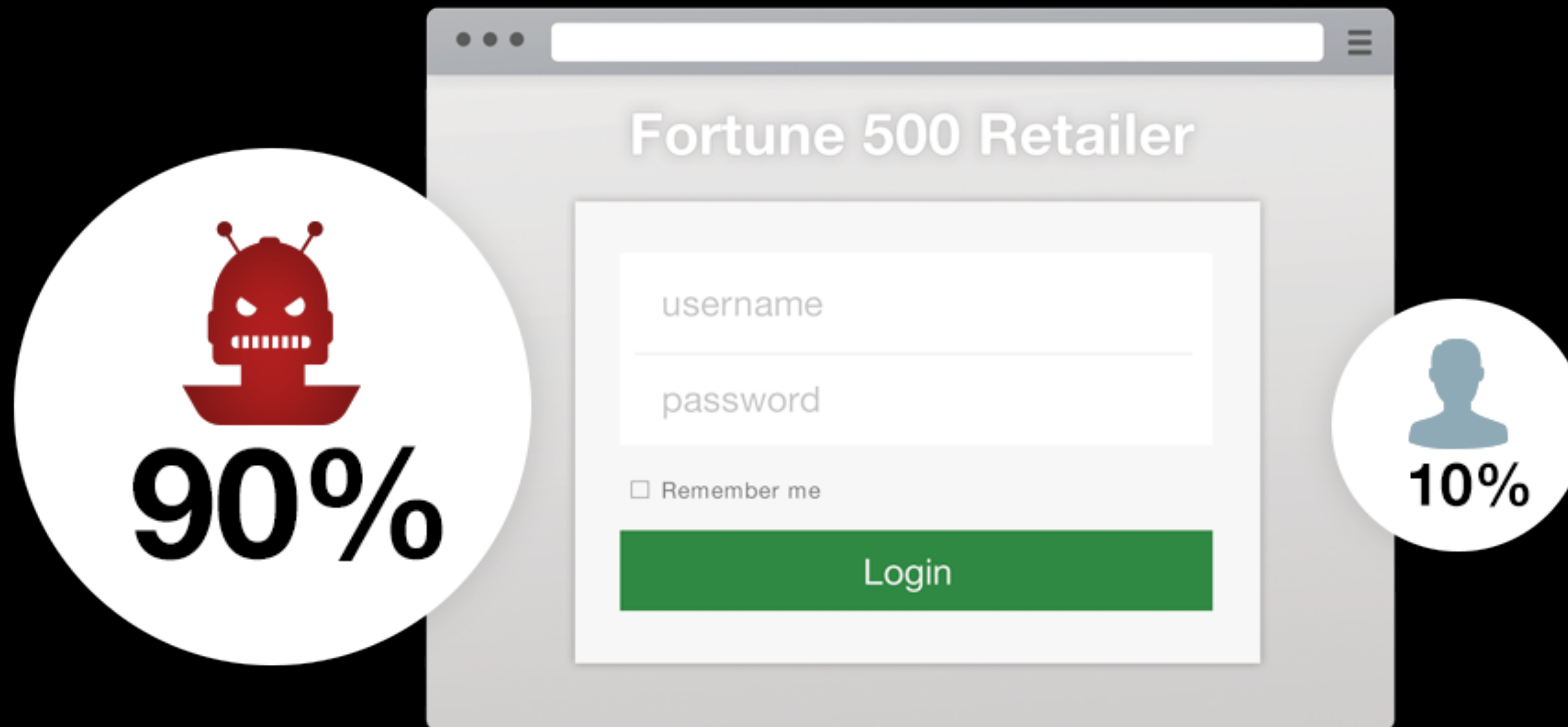
- Pay-per-click model
- \$23B in annual revenue
- >\$100K per minute
- One main incentive
- Many methods

# Click bots





# Many bots target login forms



# Account checking bots

The screenshot shows a web application interface for account checking bots. The interface is divided into several sections:

- Top Bar:** Contains 'Start' and 'Abort' buttons, a 'Site' dropdown menu with the URL `https://api.steampowered.com/ISteamOAuth2/GetTokenWithCredentials/v0001`, a 'Switch Site' dropdown, a 'Progress' bar at 0%, and a 'List' dropdown set to 'combosteam'.
- Settings Sidebar:** A vertical menu on the left with options: 'General' (highlighted with a red circle), 'HTTP Header', 'Proxy Settings', 'Fake Settings', and 'Keywords'.
- Site Settings:** Includes 'Timeout (s): 15', 'Bot relaunch delay (s): 5', and a checkbox for 'Resolve Hostname'.
- Combo Settings:** Features a '<USER>:<PASS> filter' dropdown set to 'Apply same rules for <USER> and <PASS>', 'Minimum Length: 6' and 'Maximum Length: 8' spinners, checkboxes for 'Letters', 'Digits', 'Alphanumeric', and 'Email', 'Forbidden Chars' and 'Allowed Chars' text boxes, checkboxes for 'Lowercase and Uppercase', 'Letter and Digit', and 'Special Character', and an '<EMAIL> filter' dropdown set to 'Must Be Email'.
- General Settings:** Includes checkboxes for 'Save automatically valid usernames and expired combos', 'Save automatically "To Check" combos', 'Annoying sound on Hit ->' (with a 'Browse' button), 'Popup Memo containing Hit debug information', 'Minimize to Tray', 'Float Statistics in Progression', and 'Detect "network lost" conditions while bruteforcing'. A 'Progression updates: 0' spinner is also present.
- Snap Shots:** Contains a checked checkbox for 'Enable Snap Shots' (with a red circle around it), a 'Load Settings from Snap Shot' button (with a red circle around it), and a 'Save Settings to Snap Shot' button.
- Images Database:** Includes a question mark icon and two buttons: 'Update Images Database from Directory' and 'Update Images Database from File'.
- Status Bar:** At the bottom, it shows 'Wordlist: combosteam.txt', '1/5927 (0%)', and a redacted area.

# Credential Stuffing at Sony (2011)

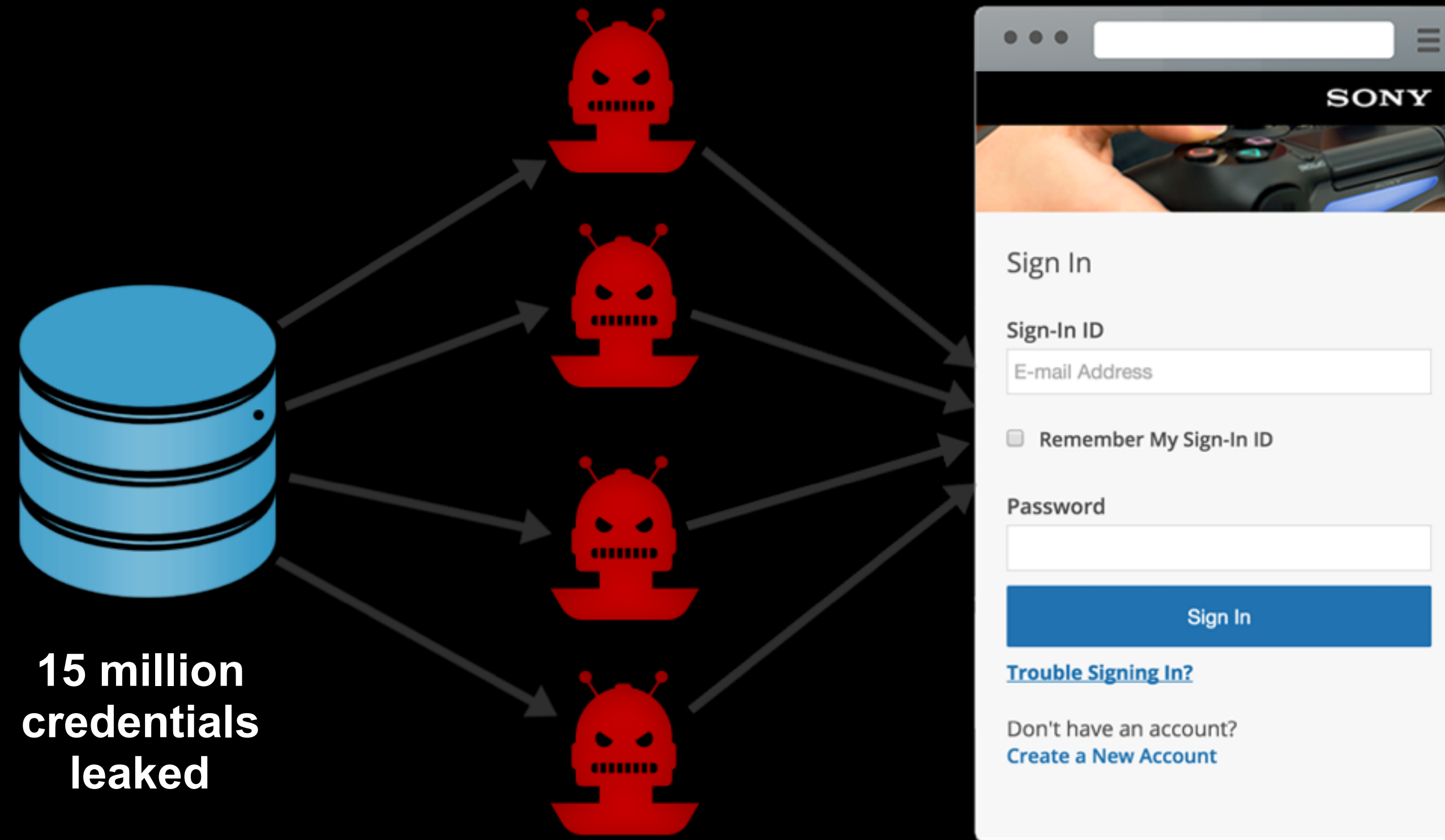


**15 million  
credentials  
leaked**

A screenshot of the Sony website's sign-in page. The page has a white background with a blue header containing the Sony logo and a navigation menu. Below the header is a sign-in form with the following elements: a 'Sign In' heading, a 'Sign-In ID' label above a text input field containing 'E-mail Address', a checkbox labeled 'Remember My Sign-In ID', a 'Password' label above another text input field, a blue 'Sign In' button, a blue link for 'Trouble Signing In?', and a link for 'Don't have an account? Create a New Account'.

93,000 matches on Sony site =  
93,000 user accounts breached

# Botnets defeat all IP-based defenses



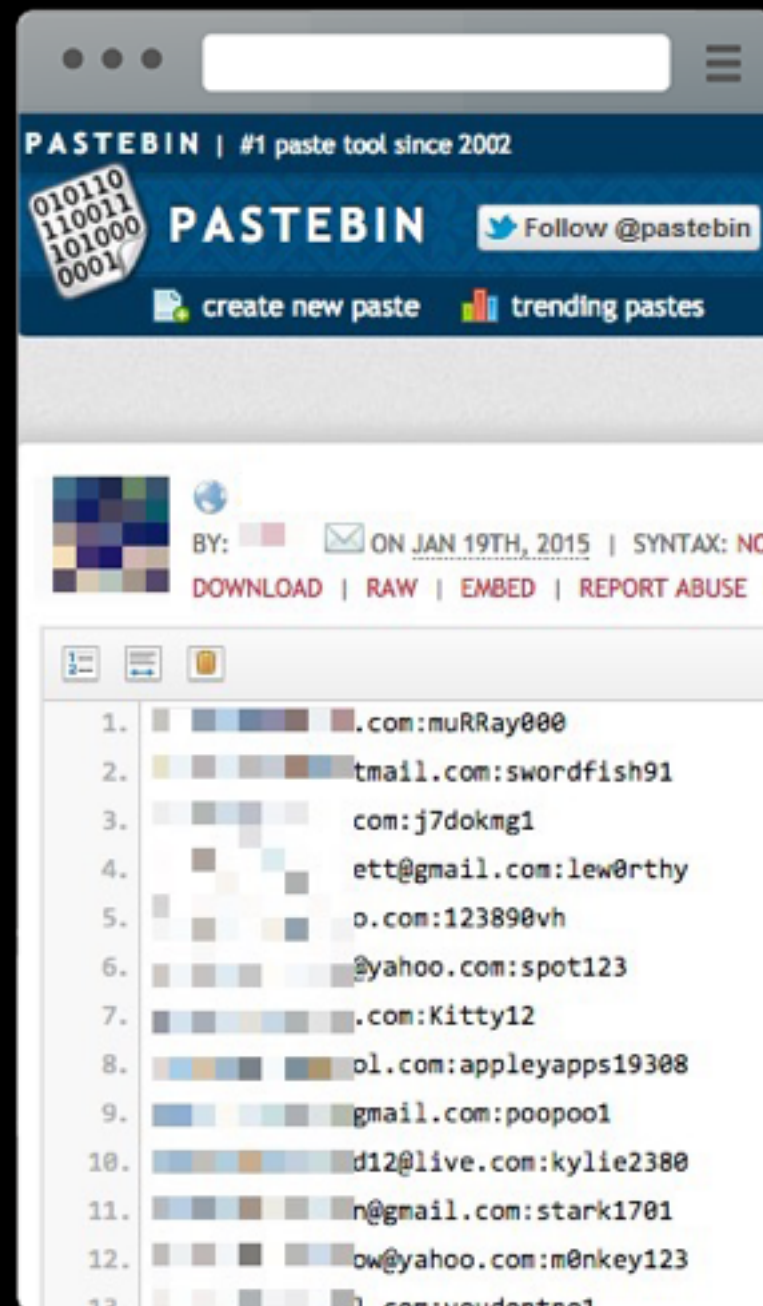
15 million  
credentials  
leaked

Botnet tests for  
password reuse

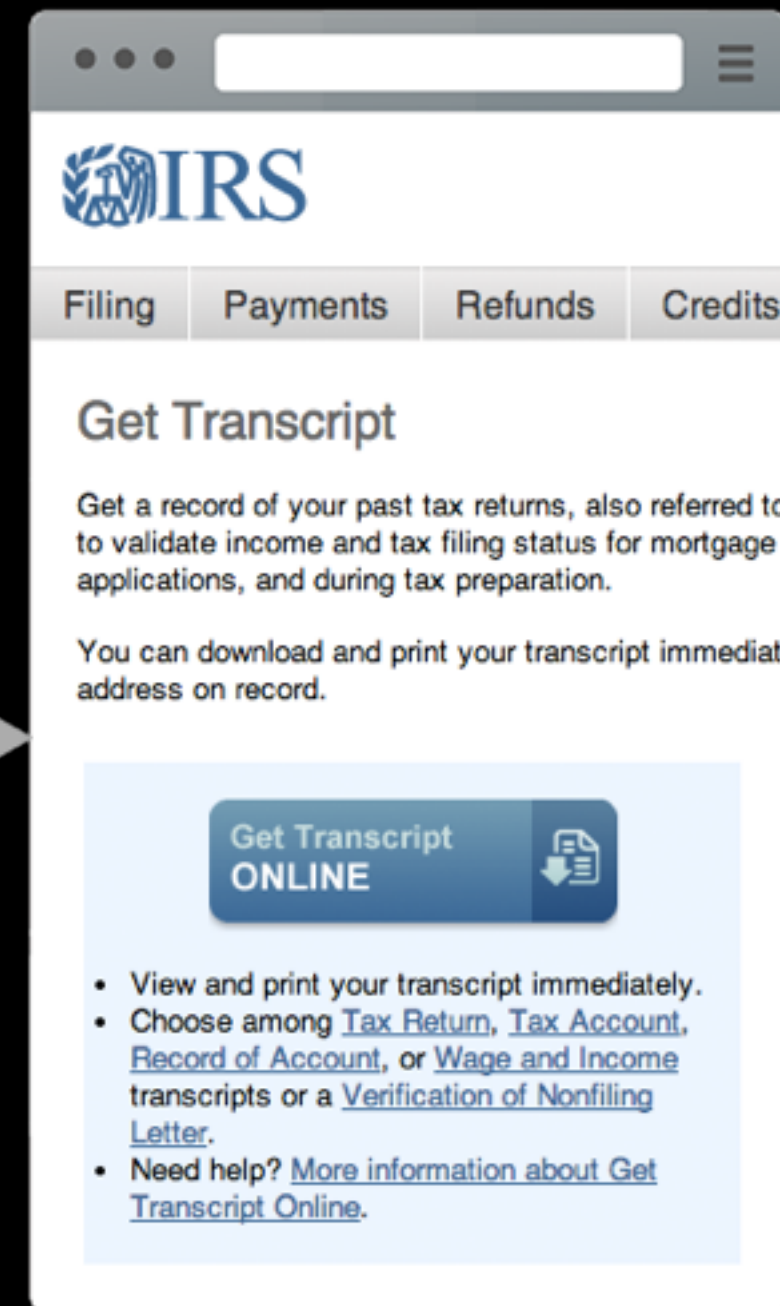
93,000 matches on Sony site =  
93,000 user accounts breached

# Tax Fraud

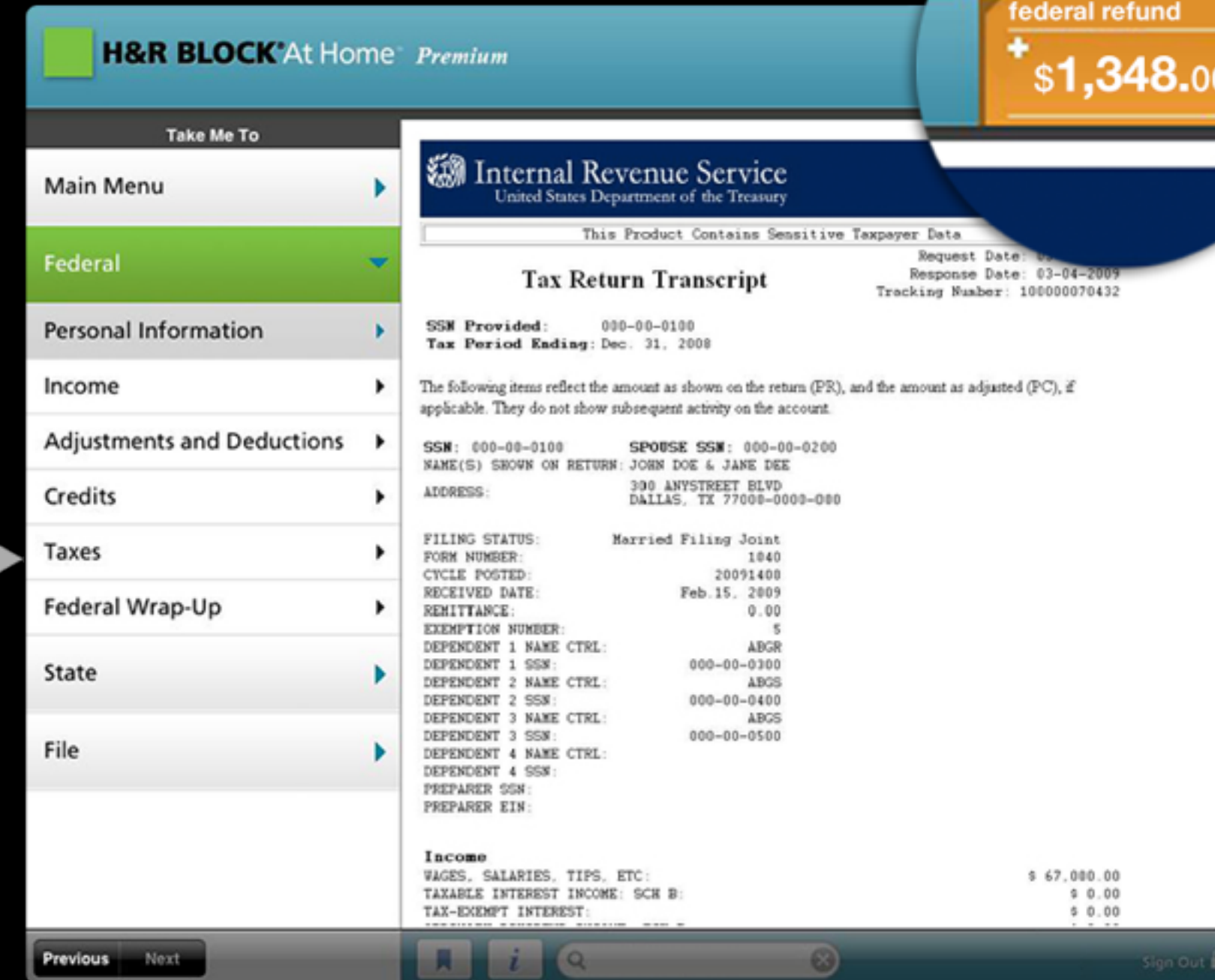
Step 4: Receive fraudulent return



Step 1: Gather “fullz” credentials from black market

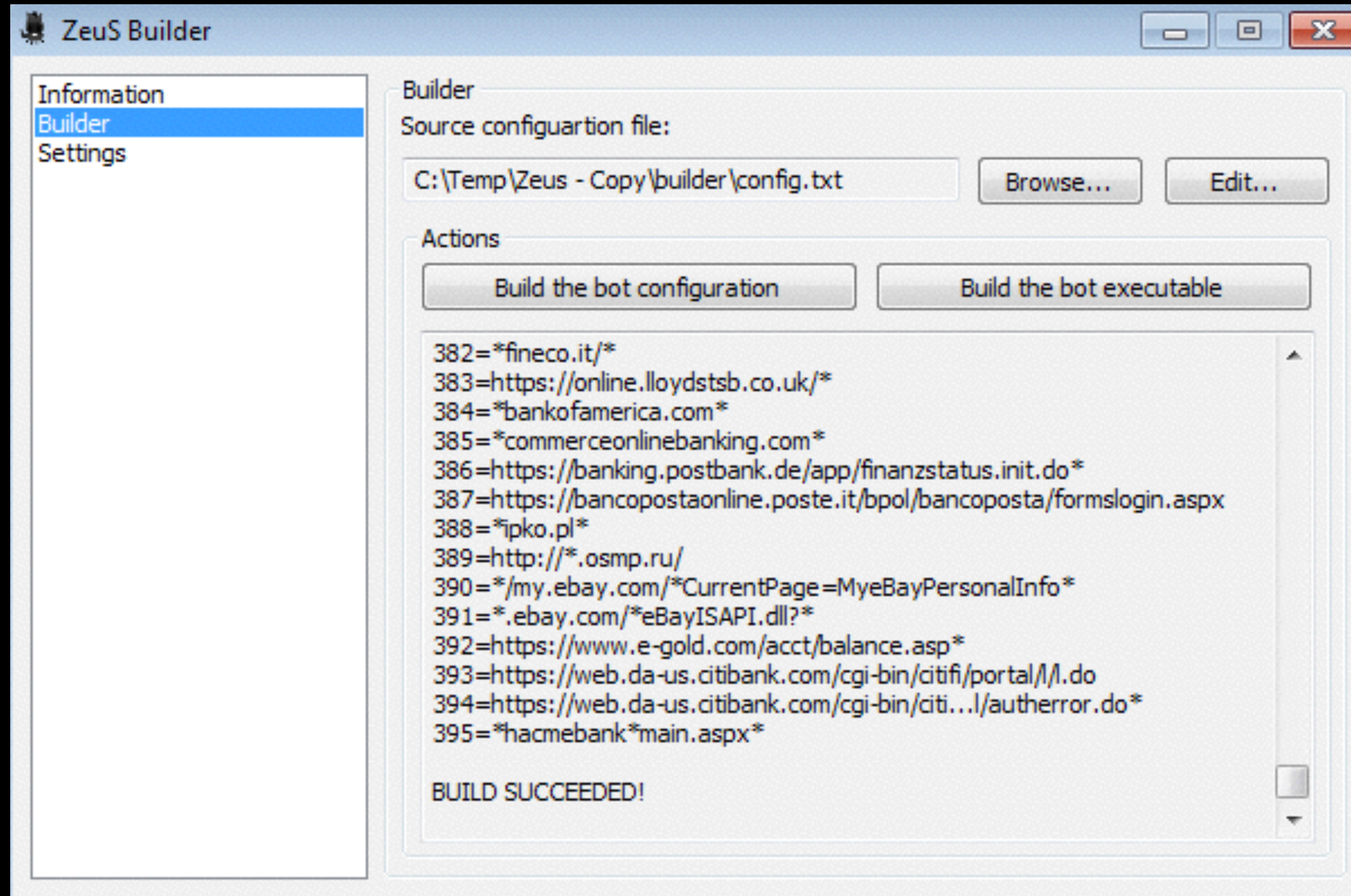


Step 2: Download tax transcripts from IRS



Step 3: Use tax transcripts to file fraudulent return in tax software

# Online Banking Fraud



# Poker bots

**Pokerbot: Settings** [Minimize] [Maximize] [Close]

Player File:  ...

**Blinds**

Buy In: 100 blinds

Min Blind: \$20k

max Blind: \$20m

**Logging**

Log Text       Log Hand History  
 Log Blinds       Log Actions  
 Log Cards       Take Screenshots

**Browser**

Browser Title:  ▼  
Browser File:  ▼

Skip this window next time the bot starts

# Ticketing bots



HOME | PRODUCTS | SUPPORT | AFFILIATE

Home

Products

Support

Affiliate

ALL THE SOFTWARES ARE MULTI-THREADED, HAVE CAPTCHA BYPASS & PROXY SUPPORT.  
INSTANT DELIVERY VIA EMAIL

## TicketMaster Spinner/Drop Checker Bot

(Works for Drop Checking, Presales, Onsale Events, everything)

Check out the Screenshots Below

**Website:** <http://www.TicketMaster.com> (Region Independent i.e it will work on all regional websites of TicketMaster e.g TicketMaster.com, TicketMaster.ca, TicketMaster.co.uk, TicketMaster.com.au etc as well as LiveNation.com)

**Bot Type:** [Tickets Spinner/Tickets Purchaser/Tickets Drop Checker](#)

### What exactly this software does?

The software allows you to reserve multiple tickets, you can do multiple searches simultaneously on one event or multiple events with just a click of a mouse. You can use it for drop checks as well as set them for presales and onsale events. It also has an option to allow you to set the bot to start at a specific time, while you are not there and the software will start at a time and grab the tickets and notify you, if the tickets match your criteria. The bot can be customized to meet your exact needs as well.

### New Exciting Features!

Grabs tickets and hold for you instantly as soon as they get dropped

Scheduler: To start searching for tickets at a given time.

Works on Onsale as well as Pre-Sale events

Grabs only particular tickets having specified section and/or row

Notify you via email/sms/sound when tickets are found

Option to automatically purchase tickets for you as soon as they are found

Robust speed!

Multiple Proxies for different threads

Order

With \*CAPTCHA Bypass

~~\$1800~~ \$990 only.

\*PS. If you are having any issues with the payment or would like to pay via any other payment method, please contact us at [TicketBots.net@Gmail.com](mailto:TicketBots.net@Gmail.com)



**Why is automation so easy?**

# All websites present an API

The image shows a browser window displaying the Amazon sign-in page. The URL is `www.amazon.com/ap/signin?_encoding=U`. The page features the Amazon logo, navigation links for "Your Account" and "Help", and a "Sign In" section. The "Sign In" section includes a form with the following elements:

- Sign In**
- What is your e-mail or mobile number?**
- E-mail or mobile number:
- Do you have an Amazon.com password?**
- No, I am a new customer.
- Yes, I have a password:
- [Forgot your password?](#)
- 

A developer tool overlay is visible at the bottom, showing the HTML structure of the page. The selected element is the email input field, with the following HTML code:

```
<input id="ap_email" name="email" value type="email" size="30" maxlength="128"
tabindex="1" autocorrect="off" autocapitalize="off">
```

The developer tool also shows the HTML structure for the password field:

```
<input id="ap_password" name="password" type="password" maxlength="1024" size=
"20" tabindex="2" onkeypress="if (typeof(displayCapsWarning) !== 'undefined') {
displayCapsWarning(event, 'ap_caps_warning', this); }" class="password">
```

**How can we stop bots?**




**Make life harder for robots with  
our own robotic defenses**

# CAPTCHA

*Wasting the world's time for 15+ years and counting*

**Require Captcha**

**Security Check**  
Please enter the text below



Can't read the text above?  
[Try another text](#) or an [audio CAPTCHA](#)

Text in the box:

[What's this?](#)

By proceeding, you agree to the [Facebook Platform policies](#)

[Continue](#) [Cancel](#)

# Every day, the world spends 17 person years solving CAPTCHAs (CMU Estimate)

## Verify Your Registration

Enter the code shown:  [More info](#)

This helps prevent automated registrations.



WORD  
VERIFICATION



enter the characters  
for the symbols shown  
in the box below:



♣ = 4 ♣ = j ♀ = d □ = n ♪ = x + = k

▷ = v 😊 = r ♖ = h ♦ = t ♣ = 7 ♞ = a

# Metal CAPTCHA

Band's name here



METAL CAPTCHA  
HEAVY/CIFTS

Band's name here



METAL CAPTCHA  
HEAVY/CIFTS

Band's name here



METAL CAPTCHA  
HEAVY/CIFTS

Band's name here



METAL CAPTCHA  
HEAVY/CIFTS

Band's name here



METAL CAPTCHA  
HEAVY/CIFTS

Band's name here



METAL CAPTCHA  
HEAVY/CIFTS

# reCAPTCHA

morning overtook

Type the two words:





# CAPTCHA beating tools

www.deathbycaptcha.com/user/login

**DEATH BY CAPTCHA**  
FASTEST DISCOUNT CAPTCHA SOLVERS

**VITARANK DISCOUNT SEO.**  
100% GUARANTEED DELIVERY.

**SAVE 10% INSTANTLY**  
USE CODE: **VRDBC** AT CHECKOUT

English   Русский   简体中文

Home   F.A.Q.   API   Order CAPTCHAs   DBC Points   Testimonials   Contact Us   Login

**STATUS: OK**

## CAPTCHA Bypass done right

With Death by Captcha you can solve any CAPTCHA. All you need to do is input the CAPTCHAs and we'll return the text. It's that easy!

Please note that our services should be used only for research projects and are strictly prohibited. Any misuse and CAPTCHA violations should be reported to the relevant authorities.

www.beatcaptchas.com/prices.html

**Beat Captchas.com**

Home   Register   Prices   Imacros Code   Contact   Login

|                  | <u>Captcha Package Size</u> | <u>Cost Per Captcha</u> | <u>Total Cost</u> |
|------------------|-----------------------------|-------------------------|-------------------|
| ➔ Captcha Prices | 1000 Images                 | \$0.008                 | \$8.00            |
| ➔ How It Works   | 5000 Images                 | \$0.007                 | \$35.00           |
| ➔ Buy Captchas   | 50000 Images                | \$0.006                 | \$300.00          |

➔ **BUY YOUR CAPTCHAS NOW!**

**But CAPTCHAs had a good idea:**

**Can't make successful attacks  
*impossible*, but you can make  
them more *difficult* and *expensive***

# **To successfully imitate a crowd, there's a lot more than IP addresses that attackers need to vary**

Screen resolution

Timezone

Browser version

Language

Fonts

Browser Plugins

Type of Pointing Device

Many other browser features

# Generalized Attack Mitigation Framework

Prevention

Real-Time  
Detection

Batch  
Detection &  
Investigation

Reactive  
Investigation

# Generalized Attack Mitigation Framework



# Need “robots” to fight robots



# Need “robots” to fight robots



Source: io9, “*Yes, Deckard’s A Replicant*” (03-23-09)

**Thank you!**

**Shuman Ghosemajumder**  
**sg@shapesecurity.com**

**@ShapeSecurity**