Protecting Your Web & Mobile Apps Against the Next Wave

H. Lane Williams

Dir. Solutions Engineering – Distributed Cloud Services

October 4, 2022

Threat Actors Keep Evolving

July 22, 1999

On this day, a computer at the University of Minnesota came under attack from a network of 114 other computers infected with a malicious script Trin00. The attack knocked out the university computer for two days.[1]

1 - https://www.technologyreview.com/2019/04/18/103186/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/

Agenda

- How bots harm businesses
- Where do Bad Actors Start?
- How to protect yourself
- Summary

Modern attacks begin with breaches and end with fraud

BREACHES, FRAUD, AND ABUSE HAVING GREATER BUSINESS IMPACT

USERNAME

****

#1

Credential attacks leading cause of extreme financial loss over past 5 years ($10BN)

78%

of orgs reported increase in customer complaints or churn due to **bot attacks** since start of pandemic

1 in 3

global consumers have experienced **fraud** in past 3 months

Churn

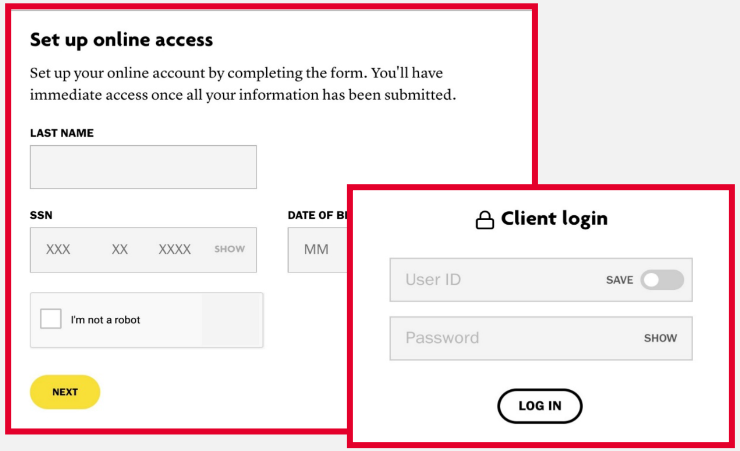
Fines

Revenue Loss

Theft

Bots blur the lines between security and fraud

Application Security

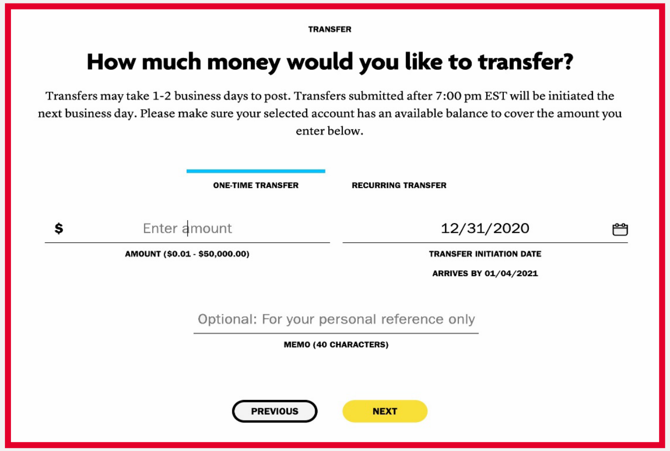


Set up online access

Set up your online account by completing the form. You'll have immediate access once all your information has been submitted.

Client login

Fraud Prevention



TRANSFER

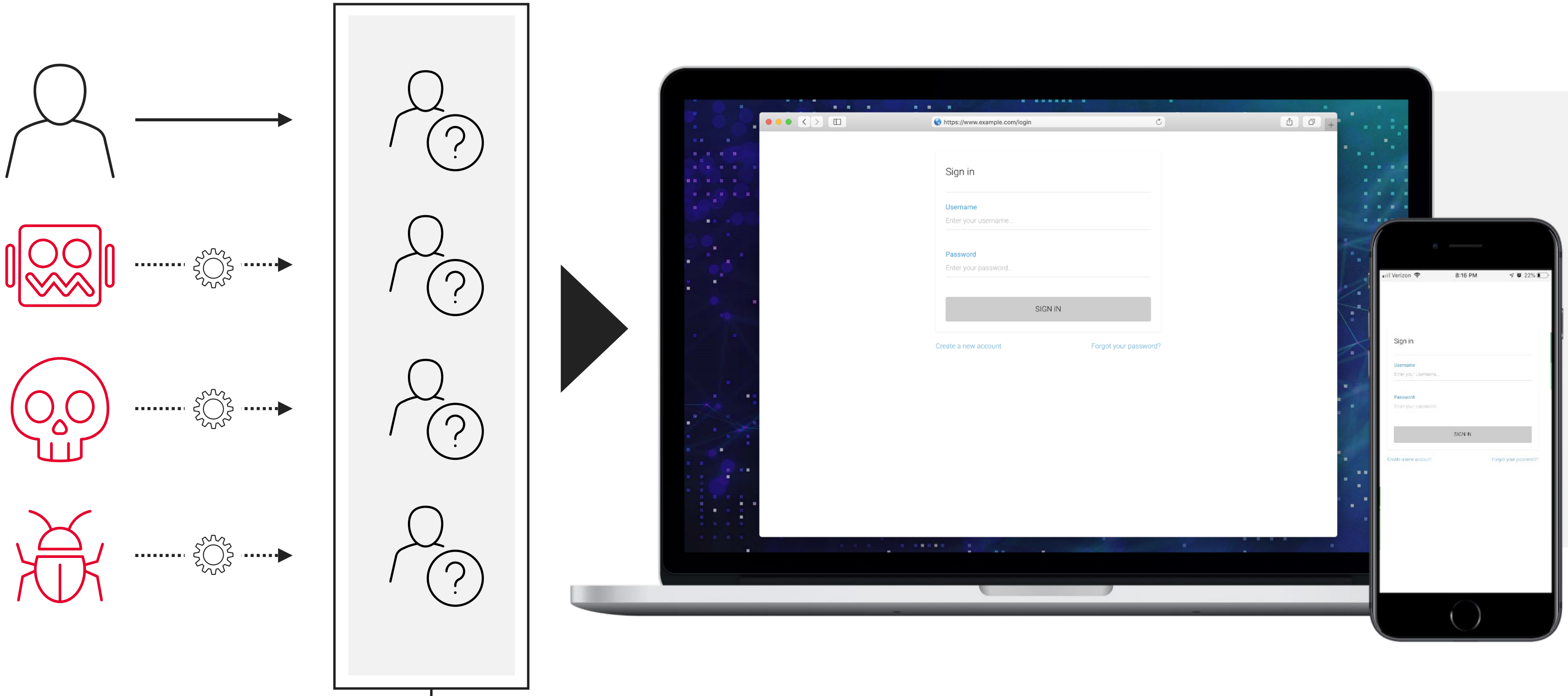
How much money would you like to transfer?

Transfers may take 1-2 business days to post. Transfers submitted after 7:00 pm EST will be initiated the next business day. Please make sure your selected account has an available balance to cover the amount you enter below.

WAF | DDoS Mitigation |
API Security Authentication

Transaction Protection | Anti-Fraud |
Identity Proofing

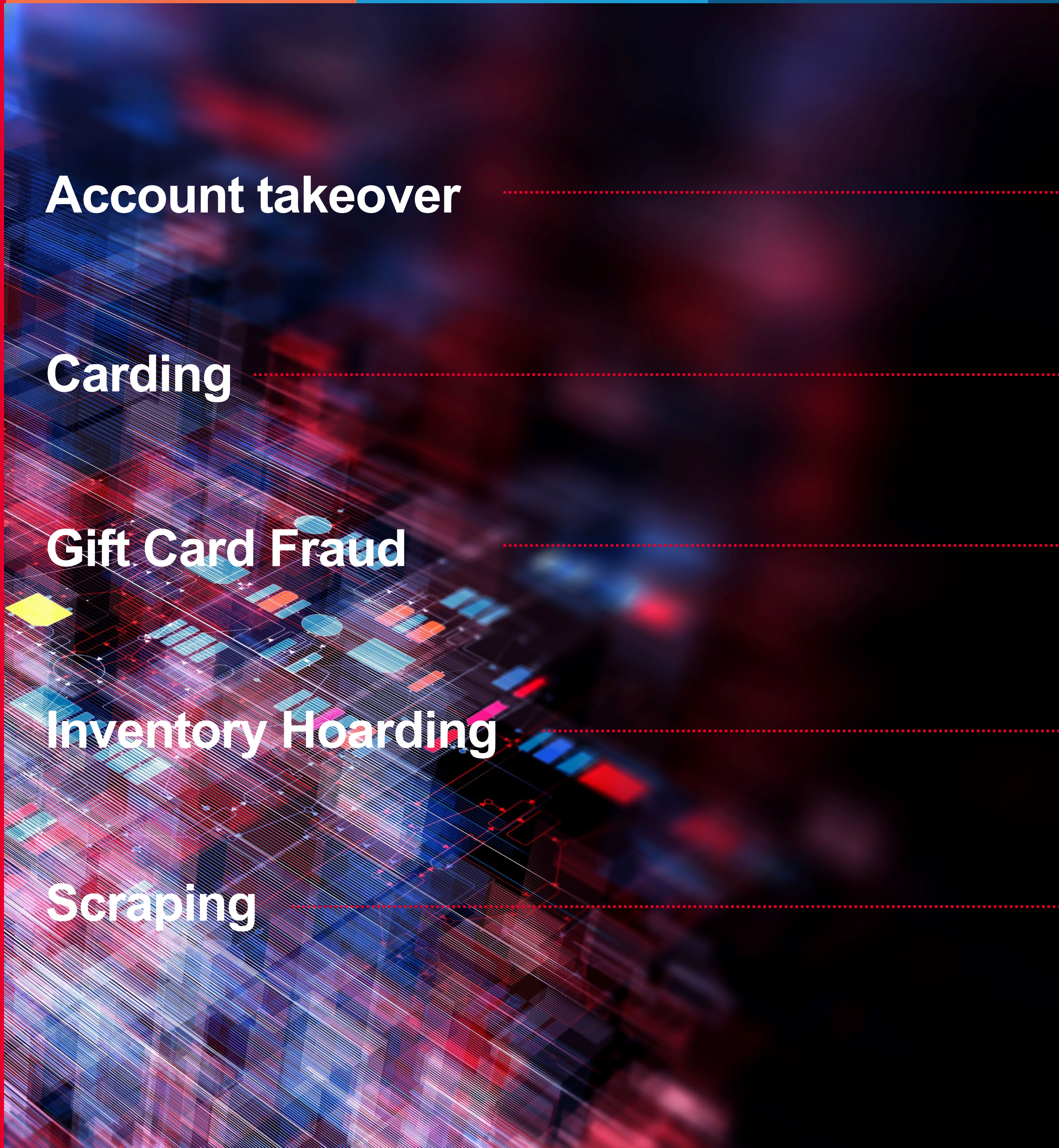
Bots are a fundamentally different type of threat



Bots look like customers and abuse inherent app functionality

> “ ”
>
> **Using our WAF and traditional firewalls** to manually block IP addresses was a **horribly ineffective** way to mitigate the very real threat posed by bots.
>
> —CISO, Major US Retailer

Bots have significant impact on the business, government and educational organizations



- Account takeover
- Carding
- Gift Card Fraud
- Inventory Hoarding
- Scraping

Bots cause harm across your organization

ATO and Fraud

$500k lost annually per organization due to credential stuffing

Manual bot blocking

10k hours manually blocking bots per year

Downtime

80% of traffic potentially unwanted automation

Poor customer experience

4 out of 5 global brands suffer churn due to bots

Agenda

⚠ How bots harm businesses

Where do Bad Actors Start?

How to protect yourself

Summary

Accelerated Attack Lifecycle

STARTS WITH UNWANTED AUTOMATION AND ENDS WITH ACCOUNT TAKEOVER AND APPLICATION FRAUD

Credentials are stolen

Data breach Phishing Keyloggers

Over 1 million stolen credentials are reported every day

Stolen credential database is built

genesis security

Financials Identity BFP Device ID

The black market has industrialized cyber crimes and fraudulent activities

Accelerated Attack Lifecycle

STARTS WITH UNWANTED AUTOMATION AND ENDS WITH ACCOUNT TAKEOVER AND APPLICATION FRAUD

Credentials
stole

Data breach Phishin

COMB (Compilation of Breaches)

- 3.2 billion unique pairs of cleartext emails and passwords
- There are ~7.9 billion people on the *entire planet*

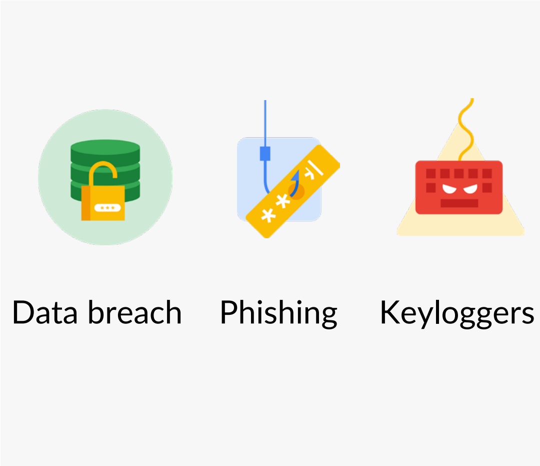
Over 1 million s
credentials are
reported every day

industrialized cyber crimes
and fraudulent activities

Accelerated Attack Lifecycle

STARTS WITH UNWANTED AUTOMATION AND ENDS WITH ACCOUNT TAKEOVER AND APPLICATION FRAUD

Credentials are stolen

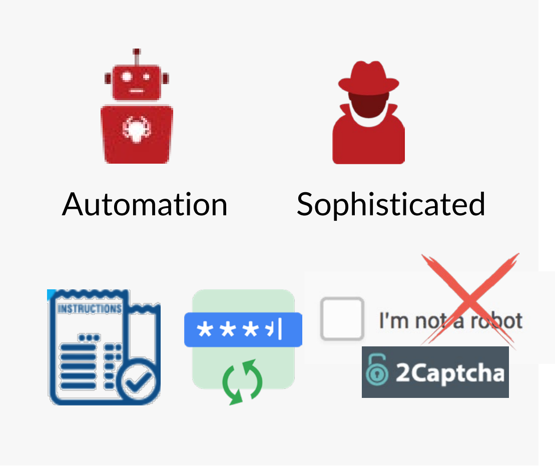


Over 1 million stolen credentials are reported every day

Stolen credential database is built

The black market has industrialized cyber crimes and fraudulent activities

Accounts are compromised

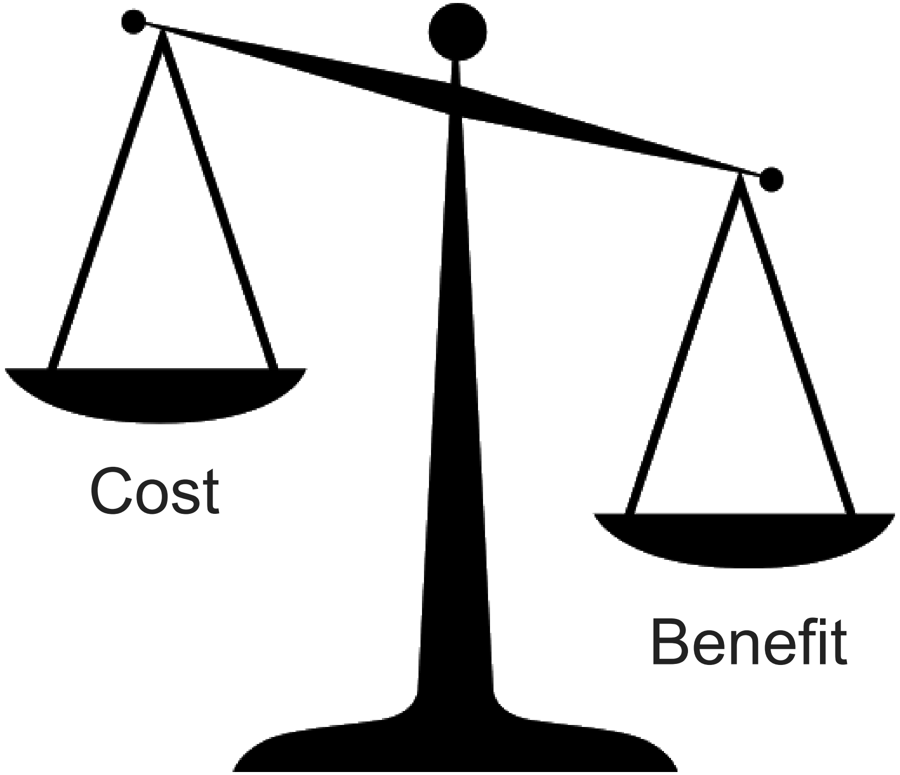


Automation, malicious bots, and manual attacks expose users and businesses to fraud

Leading to fraud and friction

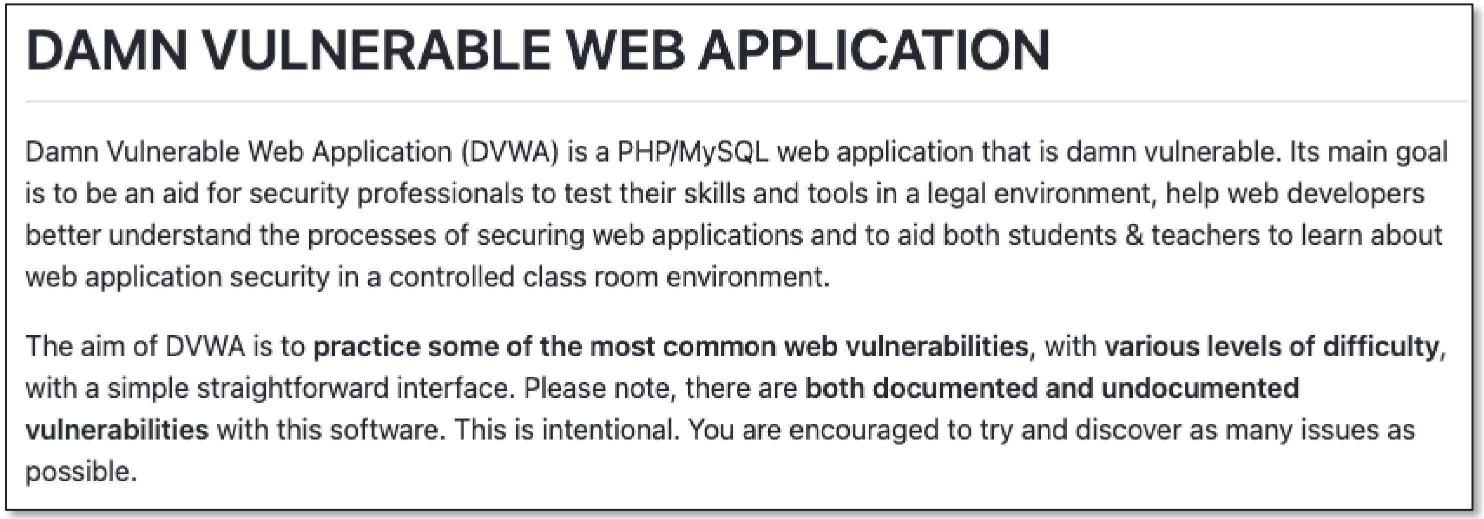
Leading to 65% increase in successful fraud attempts from 2019 to 2020

Maintaining the Balancing Act



- For the threat actor, it is a cost-benefit analysis.
- If the value outweighs the cost, the attack continues and evolves

Planning & Executing a Bot Attack



DAMN VULNERABLE WEB APPLICATION

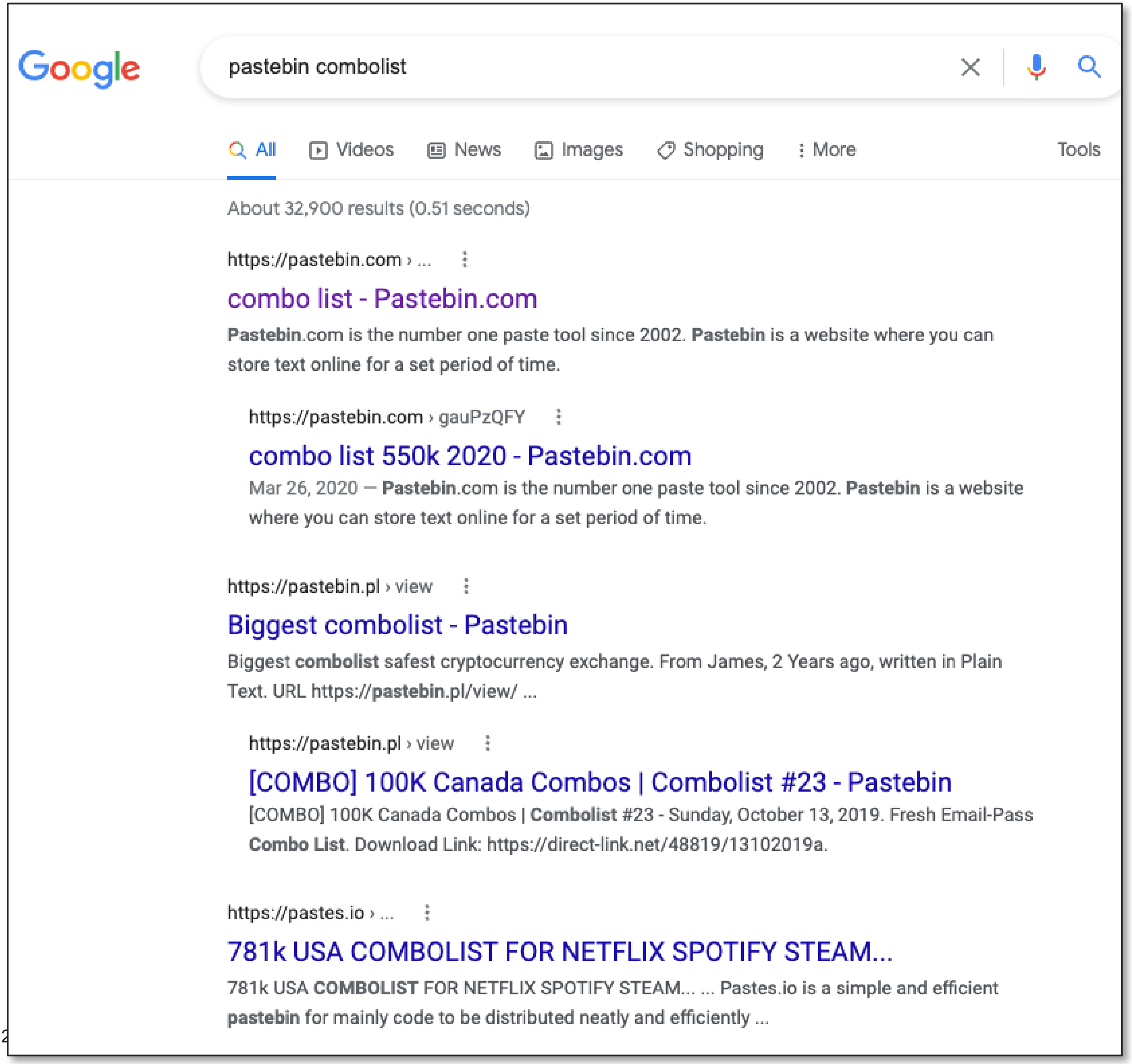
Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface. Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

https://github.com/digininja/DVWA

- DISCLAIMER
  - **Use any newfound knowledge for good!**
  - **Tools like DVWA are available to sharpen your skills.**

Planning & Executing a Bot Attack



pastebin combolist

About 32,900 results (0.51 seconds)

https://pastebin.com › ...

combo list - Pastebin.com

Pastebin.com is the number one paste tool since 2002. **Pastebin** is a website where you can store text online for a set period of time.

https://pastebin.com › gauPzQFY

combo list 550k 2020 - Pastebin.com

Mar 26, 2020 — **Pastebin**.com is the number one paste tool since 2002. **Pastebin** is a website where you can store text online for a set period of time.

https://pastebin.pl › view

Biggest combolist - Pastebin

Biggest **combolist** safest cryptocurrency exchange. From James, 2 Years ago, written in Plain Text. URL https://**pastebin**.pl/view/ ...

https://pastebin.pl › view

[COMBO] 100K Canada Combos | Combolist #23 - Pastebin

[COMBO] 100K Canada Combos | **Combolist** #23 - Sunday, October 13, 2019. Fresh Email-Pass **Combo List**. Download Link: https://direct-link.net/48819/13102019a.

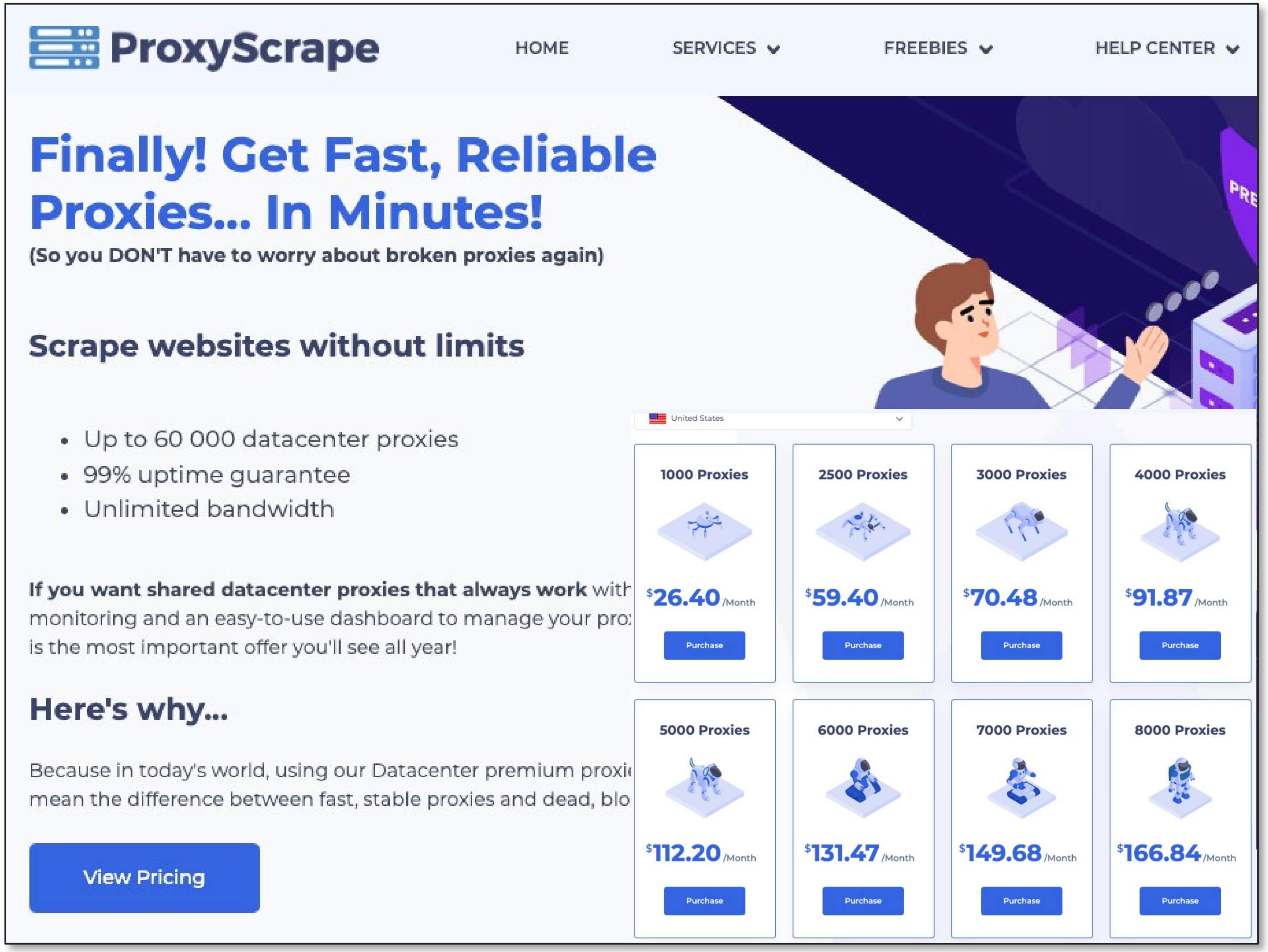
https://pastes.io › ...

781k USA COMBOLIST FOR NETFLIX SPOTIFY STEAM...

781k USA **COMBOLIST** FOR NETFLIX SPOTIFY STEAM... ... Pastes.io is a simple and efficient **pastebin** for mainly code to be distributed neatly and efficiently ...

- Get list of username/password pairs
  - **Pastebin, purchase on the Dark Web, many other places**

Planning & Executing a Bot Attack



ProxyScrape

HOME SERVICES FREEBIES HELP CENTER

Finally! Get Fast, Reliable Proxies... In Minutes!

(So you DON'T have to worry about broken proxies again)

Scrape websites without limits

- Up to 60 000 datacenter proxies
- 99% uptime guarantee
- Unlimited bandwidth

If you want shared datacenter proxies that always work with monitoring and an easy-to-use dashboard to manage your pro: is the most important offer you'll see all year!

Here's why...

Because in today's world, using our Datacenter premium proxi mean the difference between fast, stable proxies and dead, blo

View Pricing

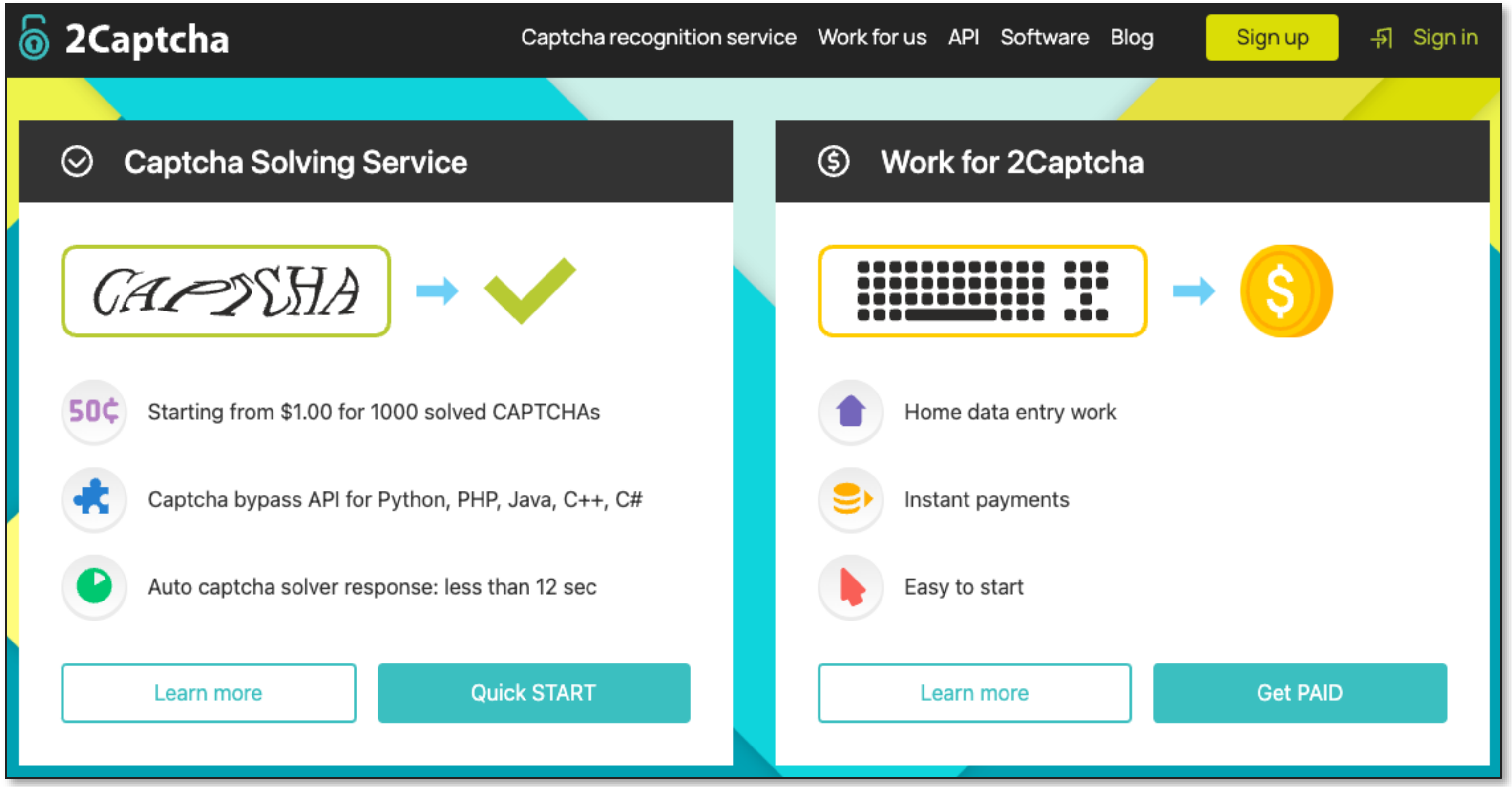
United States

1000 Proxies	2500 Proxies	3000 Proxies	4000 Proxies
$26.40 /Month	$59.40 /Month	$70.48 /Month	$91.87 /Month
Purchase	Purchase	Purchase	Purchase

5000 Proxies	6000 Proxies	7000 Proxies	8000 Proxies
$112.20 /Month	$131.47 /Month	$149.68 /Month	$166.84 /Month
Purchase	Purchase	Purchase	Purchase

- Access a Proxy Network
  - **ProxyScrape, HideMyName, Spys.One, Geonode and others**

Planning & Executing a Bot Attack



Captcha Solving Service

Starting from $1.00 for 1000 solved CAPTCHAs

Captcha bypass API for Python, PHP, Java, C++, C#

Auto captcha solver response: less than 12 sec

Work for 2Captcha

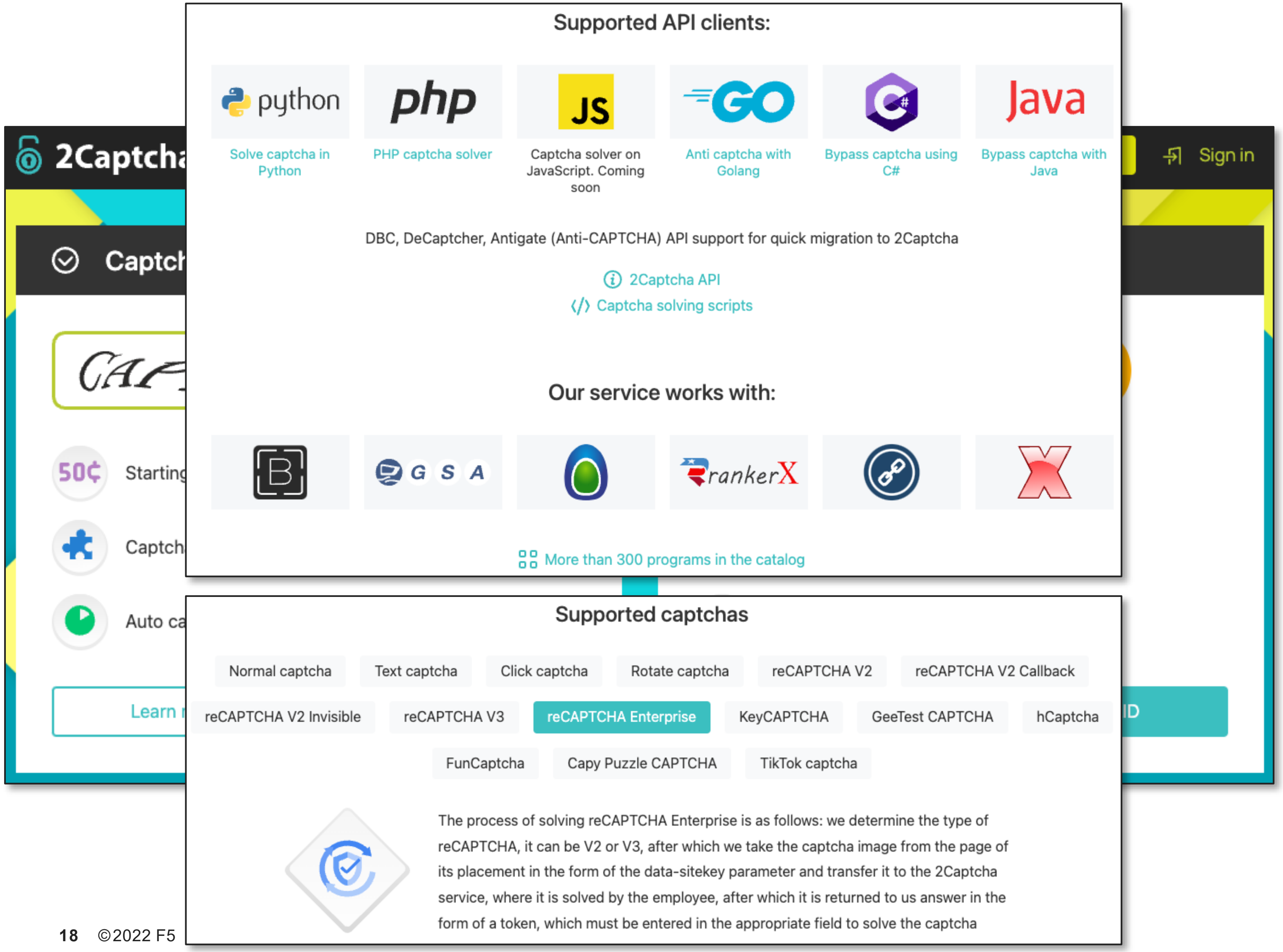
Home data entry work

Instant payments

Easy to start

- Get a CAPTCHA Solving Service
  - **2Captcha, DeathbyCaptcha, Endcaptcha, CaptchaSniper and others**
  - **All these services are API driven and can solve most all captchas**

Planning & Executing a Bot Attack



Supported API clients:

Solve captcha in Python

PHP captcha solver

Captcha solver on JavaScript. Coming soon

Anti captcha with Golang

Bypass captcha using C#

Bypass captcha with Java

DBC, DeCaptcher, Antigate (Anti-CAPTCHA) API support for quick migration to 2Captcha

2Captcha API

Captcha solving scripts

Our service works with:

More than 300 programs in the catalog

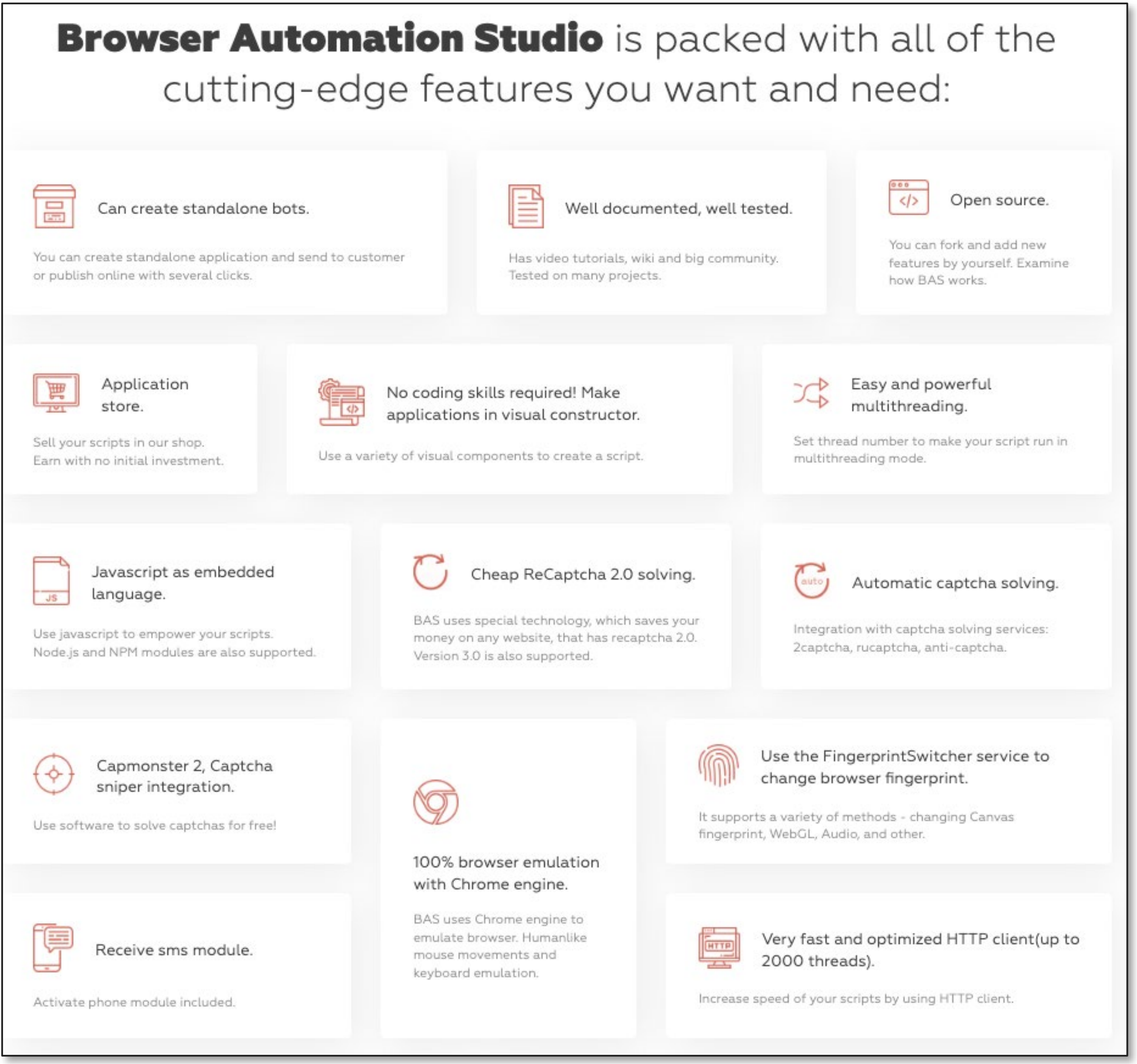
Supported captchas

Normal captcha | Text captcha | Click captcha | Rotate captcha | reCAPTCHA V2 | reCAPTCHA V2 Callback | reCAPTCHA V2 Invisible | reCAPTCHA V3 | reCAPTCHA Enterprise | KeyCAPTCHA | GeeTest CAPTCHA | hCaptcha | FunCaptcha | Capy Puzzle CAPTCHA | TikTok captcha

The process of solving reCAPTCHA Enterprise is as follows: we determine the type of reCAPTCHA, it can be V2 or V3, after which we take the captcha image from the page of its placement in the form of the data-sitekey parameter and transfer it to the 2Captcha service, where it is solved by the employee, after which it is returned to us answer in the form of a token, which must be entered in the appropriate field to solve the captcha

- Get a CAPTCHA Solving Service
  - **2Captcha, DeathbyCaptcha, Endcaptcha, CaptchaSniper and others**
  - **All these services are API driven and can solve most all captchas**

Planning & Executing a Bot Attack



Browser Automation Studio is packed with all of the cutting-edge features you want and need:

Can create standalone bots.

You can create standalone application and send to customer or publish online with several clicks.

Well documented, well tested.

Has video tutorials, wiki and big community. Tested on many projects.

Open source.

You can fork and add new features by yourself. Examine how BAS works.

Application store.

Sell your scripts in our shop. Earn with no initial investment.

No coding skills required! Make applications in visual constructor.

Use a variety of visual components to create a script.

Easy and powerful multithreading.

Set thread number to make your script run in multithreading mode.

Javascript as embedded language.

Use javascript to empower your scripts. Node.js and NPM modules are also supported.

Cheap ReCaptcha 2.0 solving.

BAS uses special technology, which saves your money on any website, that has recaptcha 2.0. Version 3.0 is also supported.

Automatic captcha solving.

Integration with captcha solving services: 2captcha, rucaptcha, anti-captcha.

Capmonster 2, Captcha sniper integration.

Use software to solve captchas for free!

100% browser emulation with Chrome engine.

BAS uses Chrome engine to emulate browser. Humanlike mouse movements and keyboard emulation.

Use the FingerprintSwitcher service to change browser fingerprint.

It supports a variety of methods - changing Canvas fingerprint, WebGL, Audio, and other.

Receive sms module.

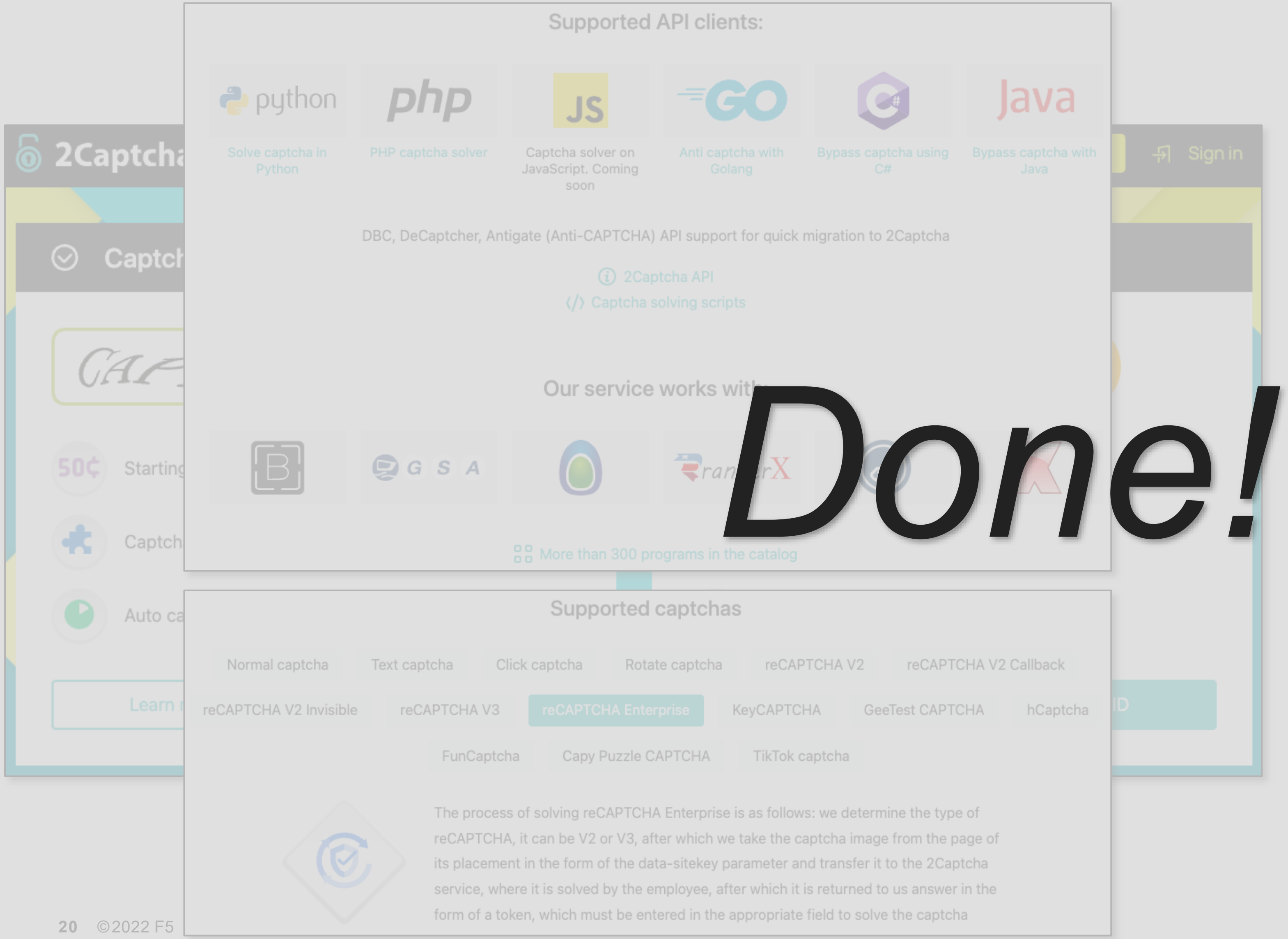
Activate phone module included.

Very fast and optimized HTTP client(up to 2000 threads).

Increase speed of your scripts by using HTTP client.

- Choose your software
  - **Selenium, OpenBullet2, Browser Automation Studio and many others**
  - **Define and test your proxies**
  - **Define the file that contains usernames and passwords**
  - **Define login success and login failure**
  - **Record username/password pairs with successful logins**

Planning & Executing a Bot Attack



Supported API clients:

Solve captcha in Python

PHP captcha solver

Captcha solver on JavaScript. Coming soon

Anti captcha with Golang

Bypass captcha using C#

Bypass captcha with Java

DBC, DeCaptcher, Antigate (Anti-CAPTCHA) API support for quick migration to 2Captcha

2Captcha API

Captcha solving scripts

Our service works wit

More than 300 programs in the catalog

Supported captchas

Normal captcha · Text captcha · Click captcha · Rotate captcha · reCAPTCHA V2 · reCAPTCHA V2 Callback · reCAPTCHA V2 Invisible · reCAPTCHA V3 · reCAPTCHA Enterprise · KeyCAPTCHA · GeeTest CAPTCHA · hCaptcha · FunCaptcha · Capy Puzzle CAPTCHA · TikTok captcha

The process of solving reCAPTCHA Enterprise is as follows: we determine the type of reCAPTCHA, it can be V2 or V3, after which we take the captcha image from the page of its placement in the form of the data-sitekey parameter and transfer it to the 2Captcha service, where it is solved by the employee, after which it is returned to us answer in the form of a token, which must be entered in the appropriate field to solve the captcha

Done!

- Get a CAPTCHA Solving Service
  - **2Captcha, DeathbyCaptcha, Endcaptcha, CaptchaSniper and others**
  - **All these services are API driven and can solve most all captchas**

Agenda

How bots harm businesses

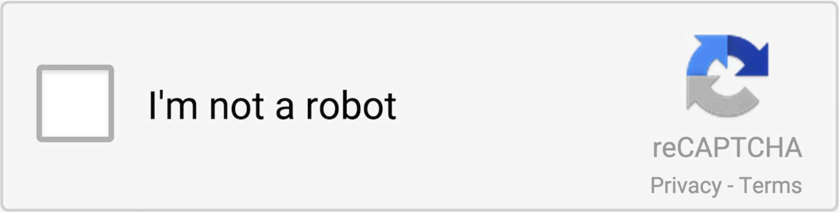
Where do Bad Actors Start?

How to protect yourself

Summary

How to Protect Yourself

- Use a CAPTCHA



- Use a CAPTCHA
  - **Yes, they are easily bypassed but they do increase the cost for attackers and makes it a little more difficult.**

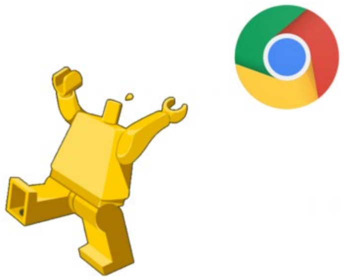
How to Protect Yourself

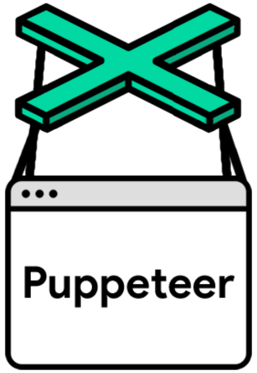
- Use a CAPTCHA
- **Rate Limit non-residential ISP’s**

- Rate limit non-residential ISP’s
  - **Most of your real consumer traffic should not be coming from AWS, Azure, Digital Ocean, Choopa or other cloud hosting providers.**

How to Protect Yourself

- Use a CAPTCHA
- Rate Limit non-residential ISP’s
- **Block or Track Headless Browsers**





- Block or Track Headless Browsers
  - **Headless Chrome and Firefox are commonly used by attackers because they are real browsers and can execute JavaScript.**
  - **Selenium and Puppeteer are popular ways to automate headless browsers**

How to Protect Yourself

- Use a CAPTCHA
- Rate Limit non-residential ISP’s
- Block or Track Headless Browsers
- **Require JavaScript on your site**

- Fingerprint your clients
  - **Somewhat simple but it does require CPU and a real browser which increases the cost for an attacker**

How to Protect Yourself

- Use a CAPTCHA
- Rate Limit non-residential ISP’s
- Block or Track Headless Browsers
- Require JavaScript on your site
- **Fingerprint Your Clients**

FingerprintJS

- Fingerprint your clients
  - **Use this as your required JavaScript**
  - **Client telemetry will help you see patterns in traffic that otherwise may be missed.**
  - **FingerprintJS on Github**

How to Protect Yourself

- Use a CAPTCHA
- Rate Limit non-residential ISP’s
- Block or Track Headless Browsers
- Require JavaScript on your site
- Fingerprint Your Clients
- **Offer Multi-Factor Authentication**

- Offer Multi-Factor Authentication
  - **A very important countermeasure that increases the difficulty and increases the cost for attackers**

How to Protect Yourself

- Use a CAPTCHA
- Rate Limit non-residential ISP’s
- Block or Track Headless Browsers
- Require JavaScript on your site
- Fingerprint Your Clients
- Offer Multi-Factor Authentication
- **Track Login Success Rate**

- Track Login Success Rate
  - **Credential stuffing attacks significantly decrease login success rate**

How to Protect Yourself

- Use a CAPTCHA
- Rate Limit non-residential ISP’s
- Block or Track Headless Browsers
- Require JavaScript on your site
- Fingerprint Your Clients
- Offer Multi-Factor Authentication
- Track Login Success Rate
- **Check user passwords against Pwned Passwords**

';--have i been pwned?

- Check user passwords against Pwned Passwords
  - **Have I Been Pwned is a site run by Troy Hunt to quickly assess if your users are still using passwords that were part of a breach.**
  - **https://haveibeenpwned.com/**

Agenda

How bots harm businesses

Where do Bad Actors Start?

How to protect yourself

Summary

Summary

- Automation is a different type of challenge and effects your business in many ways
- Understand how your attackers are targeting your web applications
- Enable additional protections for your web applications

ATO and Fraud

96% reduction in credential stuffing attacks

Manual bot blocking

40% reduction in time spent configuring custom rules and IP blacklisting

Downtime

80% reduction in unwanted bot traffic

Poor customer experience

88% reduction in account lockouts