Einblicke in den Kaninchenbau des Dark Web

WAS IST DAS DARK WEB UND WIE KANN MAN DARAUF ZURGREIFEN?

Stephan Schulz

Senior Solutions Engineer - Security

Agenda

- What is the “Dark Web”?
- What can you find
- Account Take Over Process and Tools
- How to access it safely
- Protecting your applications

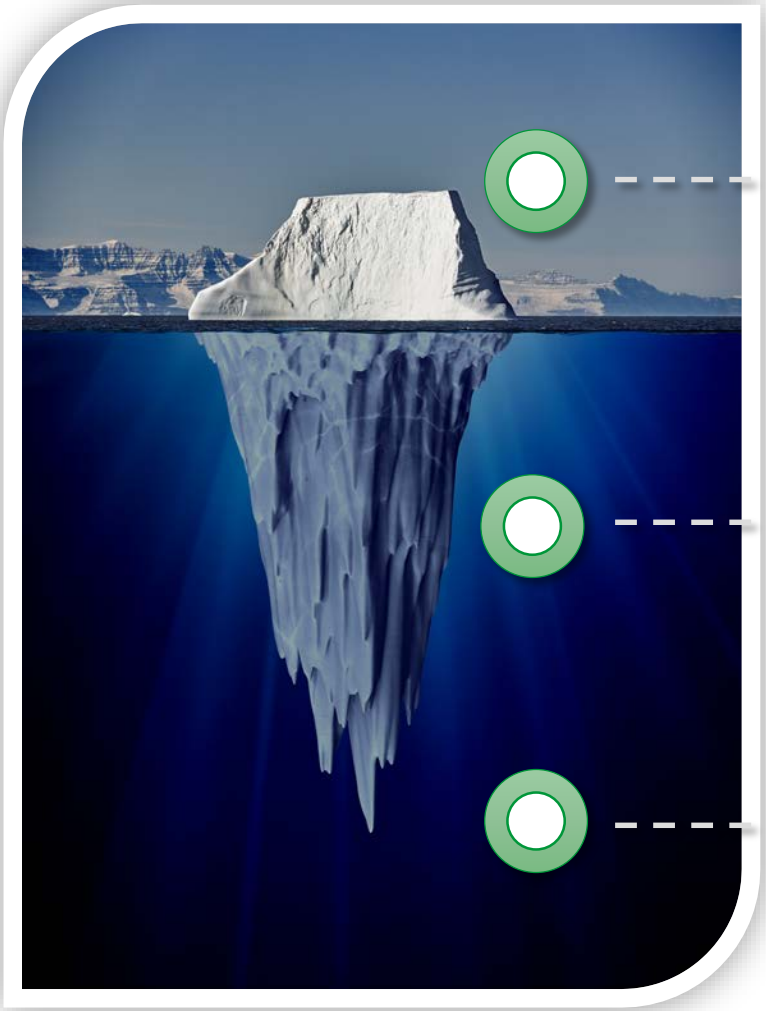
What is the “Dark Web”

The “Dark Web” Defined

“The dark web is the WWW content that exists on darknets: overlay networks… Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines…”

-- Wikipedia

The “Dark Web” Defined



Surface Web

- Accessible to all
- Public websites

Deep Web

- Unindexed content
- Corporate, Financial & Medical
- Cloud storage

Dark Web

- Private Communication
- Hidden Services
- Accessed via The Onion Router (TOR)

The “Dark Web” Defined

- The term ”Dark Web” is most often used in a broad and generic fashion to apply any place where I can find bad or illegal items or information can be found.
  - Including the follow items:
    - Public/Semi-Private forums and subgroups
    - Public e-commerce platforms
    - Phish links and content
    - Dark Markets
- A dark web user is almost always portraited as a secret member of the hoodie and Matrix fan club and sometimes with their appreciation for Guy Fawkes masks

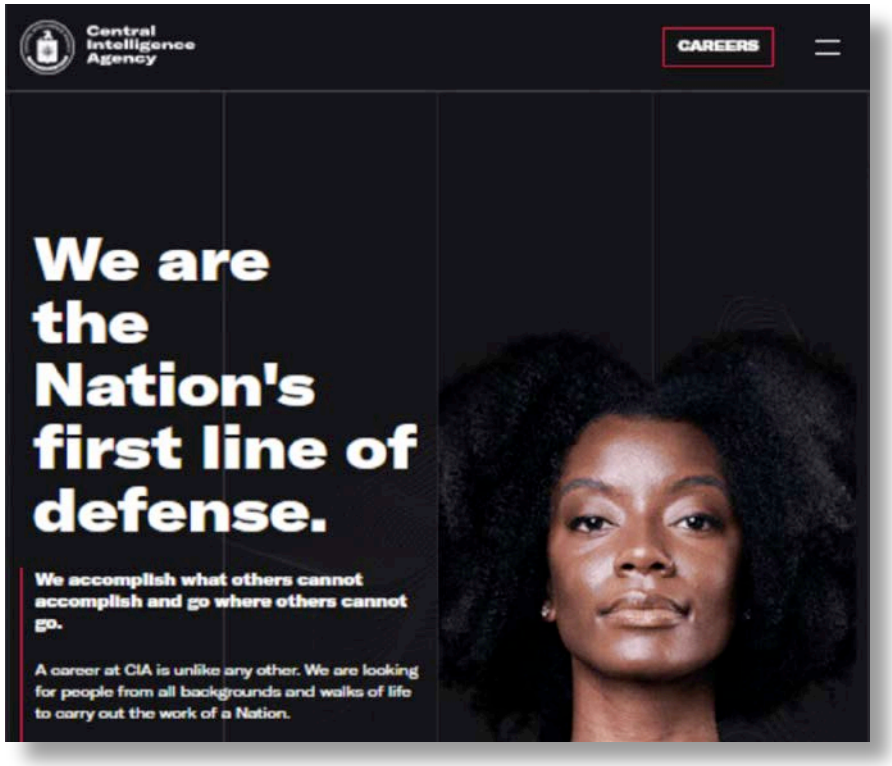
What can you find

TOR… Its not all bad

WHILE YOU MIGHT EXPECT A LONG LIST OF BAD AND ILLEGAL ITEMS LETS START ON A MORE POSITIVE NOTE

Legitimate Dark Web Content

- News – Organizations such as BBC, ProPublica & NY Times
- Secure Email and File Sharing such as ProtonMail and SecureDrop
- Bitcoin and other Cryptocurrency wallets and services.
- Search Engines and Social media – DuckDuckGo and Facebook, yep they are there too
- CIA – They keep a contact page there I’m guessing just incase



Bad items aren’t limited to the Dark Web

WE’VE SEEN MORE AND MORE SERVICE OFFERING THESE ITEMS DIRECTLY ON THE WEB

Public Sites

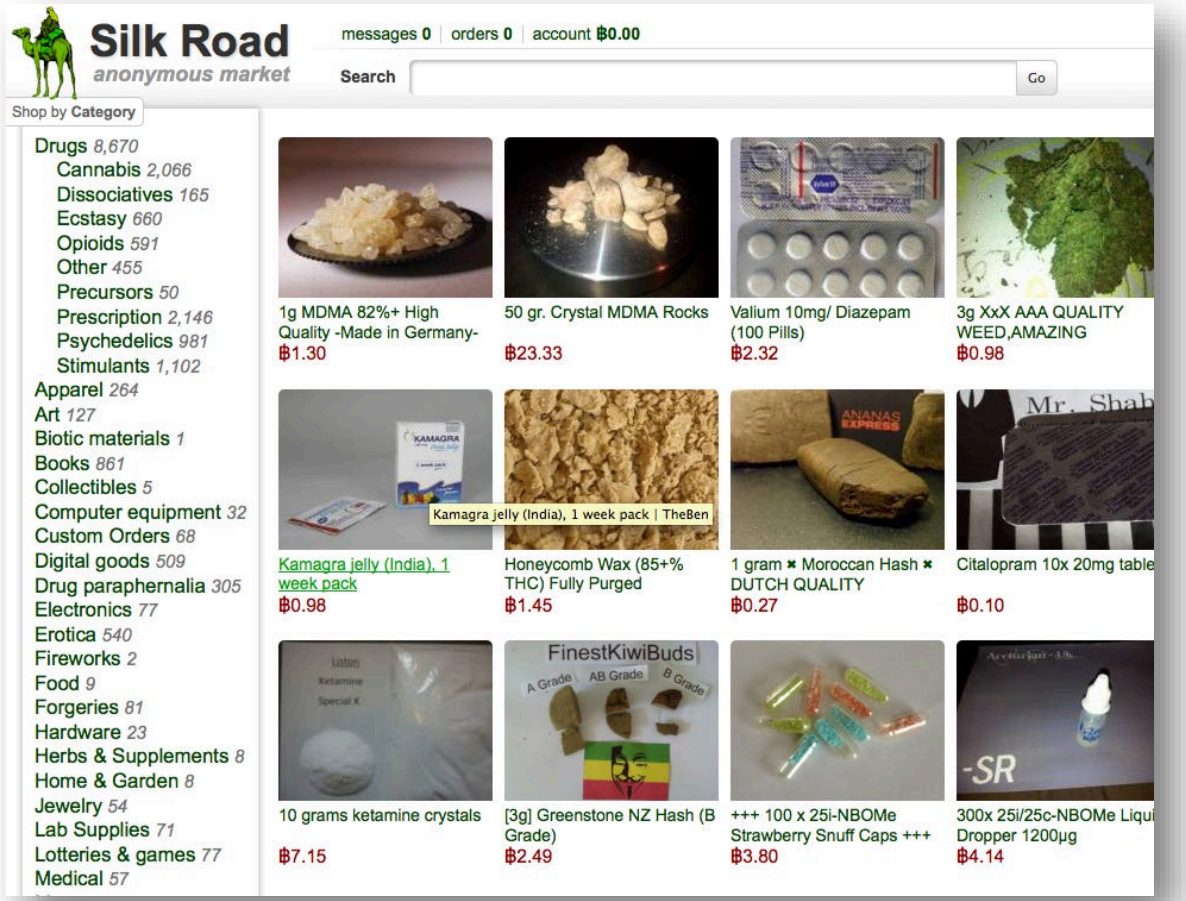
- Reddit r/ShoppingBay
- Forums such as Nulled or Cracked
- Shoppy, Sellix, eBay, AliExpress Stores
- Aggregators, Discord and Telegram channels

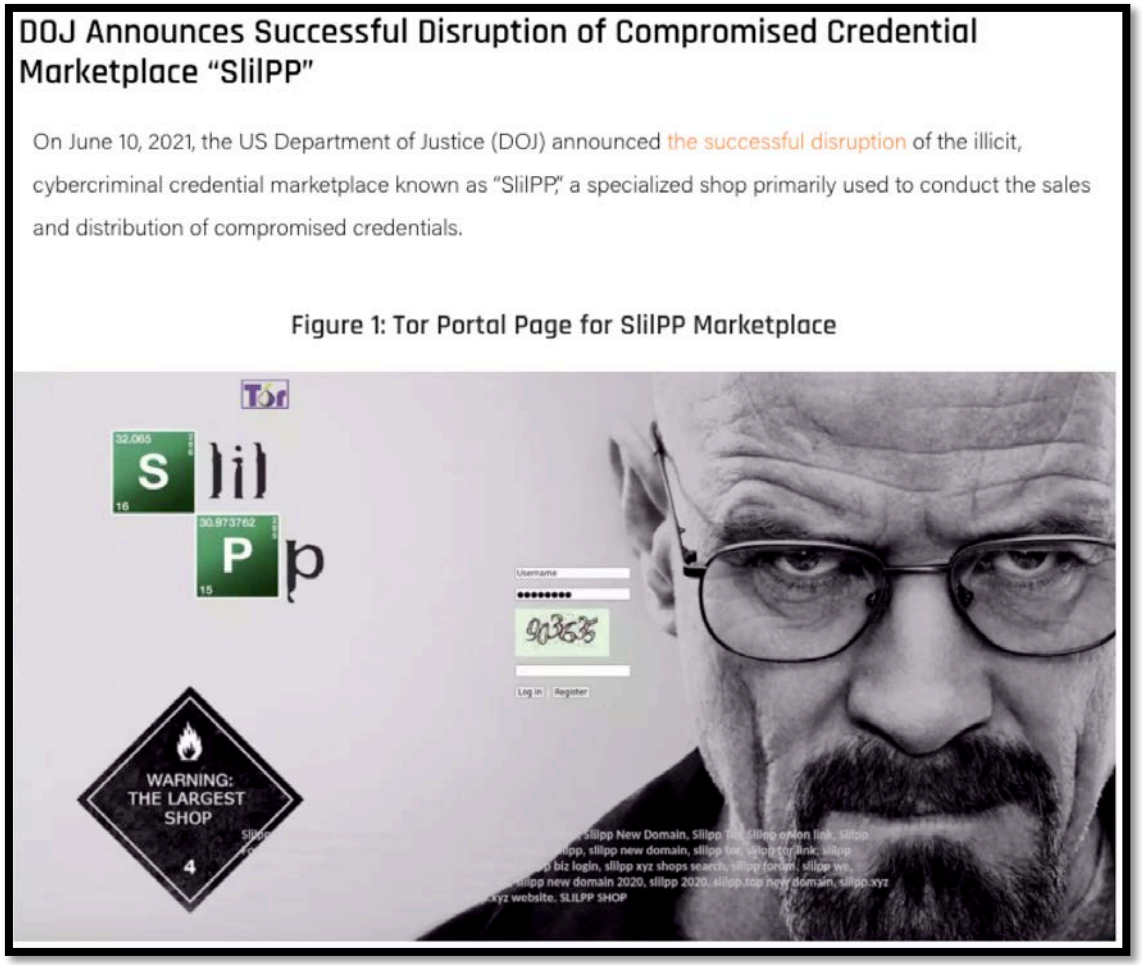
Dark Web Sites

- Base69 – Account Focused
- CanadaHQ – Multiple Items
- Info77 – Information lookup
- SRV11 – Credential Stuffing Service

Sites come and go…

ANOTHER ONE BITES THE DUST





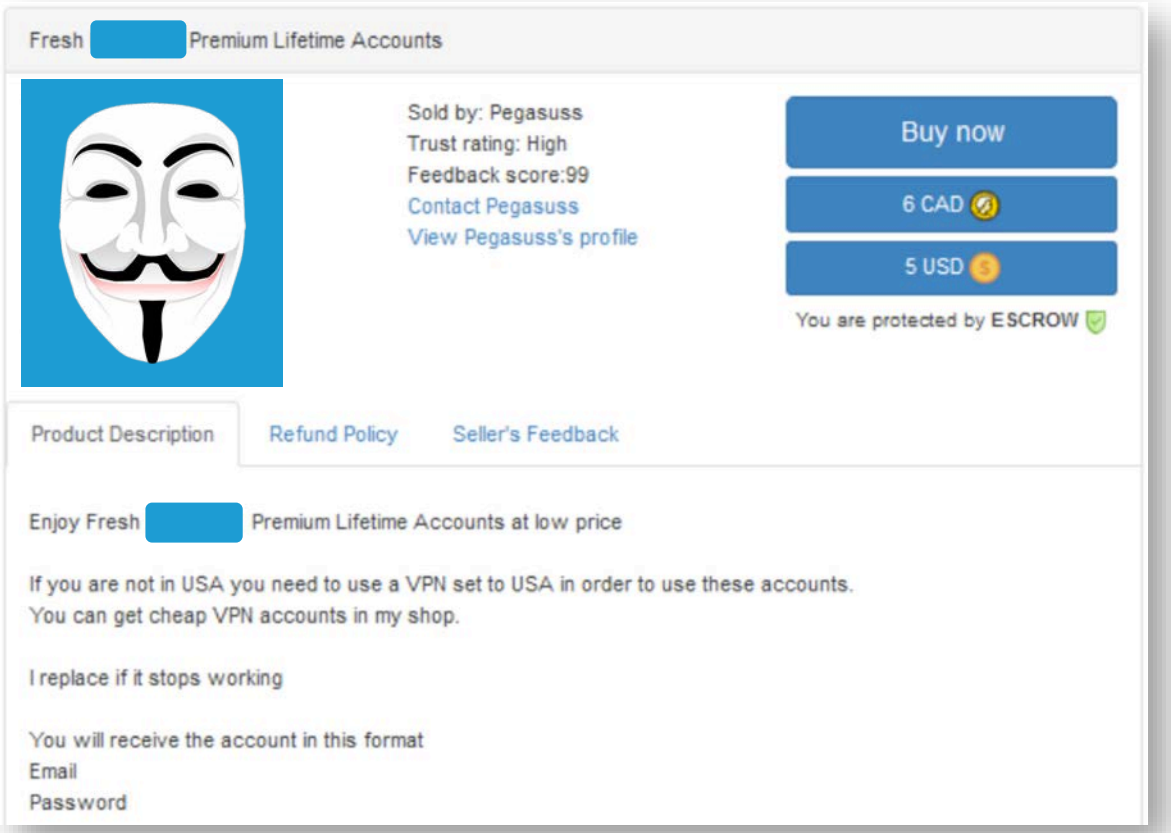
The bad…

Accounts	• Streaming Services, Food and related services, subscriptions, retail stores, social media, email and everything in between
Financial	• Bank Logins • Credit Scores and Full PII profiles • Credit card and payment services
Services	• Custom phishing sites or credential stuffing attack creation • Credential stuffing and credit card validation • Retail refunding services
Information	• Step by step how to execute various scams and attacks • Collaborate on how to defeat various security measures • Public and private attack tools
Physical Goods	• Creation of fake credentials (digital and physical) • Drugs • Weapons

Example: Accounts For Sale

Balance	Points	Name	Type	Country State Zip	CC	Bank	Info	Last order	Mail domain	Uploaded	Seller	$Price
N\A	101111.00	MARGARET	N\A	N\a MA 02122	N\A	N\A	N\A	N\A	@comcast.net	17 Mar 2021	Bunny	52
N\A	71413.00	N\A	N\A	N\a	N\A	N\A	Points = Miles | ZIP: N\A	N\A	@comcast.net	17 Mar 2021	Cr4sh	72.91
N\A	58653.00	N\A	N\A	N\a	N\A	N\A	Points = Miles | ZIP: N\A	N\A	@comcast.net	17 Mar 2021	Cr4sh	60.15
N\A	97695.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@gmail.com	17 Mar 2021	Cr4sh	98.5
N\A	159739.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@gmail.com	17 Mar 2021	Cr4sh	160.54
N\A	53697.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@gmail.com	17 Mar 2021	Cr4sh	54.5
N\A	56984.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@gmail.com	17 Mar 2021	Cr4sh	57.78
N\A	157035.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@gmail.com	17 Mar 2021	Cr4sh	157.84
N\A	81936.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@gmail.com	17 Mar 2021	Cr4sh	82.74
N\A	195715.00	N\A	N\A	N\a	N\A	N\A	ZIP: N\A	N\A	@yahoo.com	17 Mar 2021	Cr4sh	196.51
1000.00	194.98	John Doe			Type: MASTERCARD LastFour: 5988 Exp: 07/2022,Type: MASTERCARD LastFour: 6732 Exp: 09/2017,Type: VISA LastFour: 1262 Exp: 12/2021,Type: MASTERCARD LastFour: 3511 Exp: 05/2017,Type: MASTERCARD LastFour: 2500 Exp: 12/2017	N\A	ZIP: 77905	N\A	@suddenlink.net	16 Mar 2021	MrSociate	153

Lifetime Video Streaming



Example: Help please…

Disneyplus Inbox

sea ruler Yesterday

to me

G'day,

This message might be a bit strange, you don't even know me, but I have a request.

I recently bought a piece of your Disneyplus account, let's say a profile, at AliExpress.
The password was [redacted]
All worked well for a few days. Now something has changed, I can't log in anymore.
The seller on AliExpress doesn't reply. Since he's got my money, he will not respond never again.

Could you be so kind to provide me with the password?

I hope you will help me,
Best regards,
Sean

Example: Financial

Bank

[redacted] Drop (NEW) CREATION - Comes with Fullz - Original SCAN of DL & Credit Bureau

Sold by: ticallian
Trust rating: High
Feedback score:96
Contact ticallian
View ticallian's profile

Buy now
200 CAD
147 USD
You are protected by ESCROW

Product Description | Refund Policy | Seller's Feedback

Highest Quality [redacted] Bank Drop with Full Info

Comes with upon Purchase:

DL SCAN Original Driver License and Credit Bureau report with SIN
User:
Password:
Email:
Security Questions:
Security Answers

Securely load EMT to this
Reship Card if you Want
Apply for Loans
Send and Receive E-Trar
Mobile Deposit Ready for

How to ship a [redacted] DEBIT BANK CARD to your drop ****APPLY ONLINE**** . 100% Works and Verified!!!!!! - Milk Out the card and make dough!

Sold by: lordfinesse
Trust rating: High
Feedback score:99
Contact lordfinesse
View lordfinesse's profile

Buy now
100 CAD
74 USD
You are protected by ESCROW

Product Description | Refund Policy | Seller's Feedback

****All Done online********EASY, SIMPLE, FAST!!!!!This guide will explain how to ship a [redacted] Debit card to your drop without having changed credit report address to your drop before hand and also without having to actually go into the bank location to identify yourself. Everything can be done from home. This is one of the easiest ways to send cards to your drops and start making money. ITS VERY EASY!

Bank

[redacted] ACCOUNT DROPS + HOW TO LOAD★★★

Sold by: cashoutallday
Trust rating: High
Feedback score:98
Contact cashoutallday
View cashoutallday's profile

Buy now
70 CAD
58 USD
You are protected by ESCROW

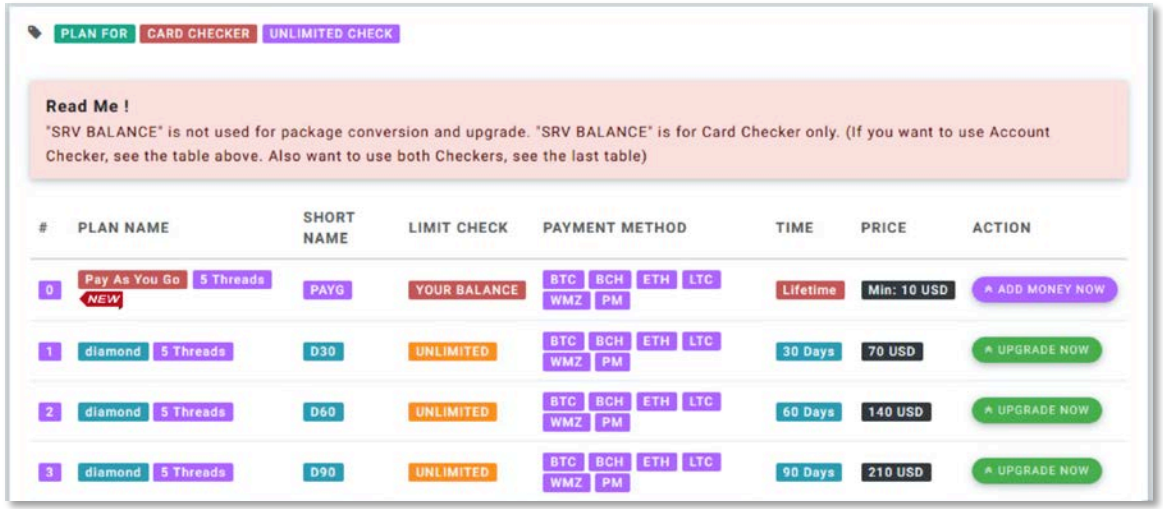
Product Description | Refund Policy | Seller's Feedback

THESE ARE VERIFIED [redacted] DROPS CREATED BY MYSELF! AGED ANYWHERE FROM 1 WEEK TO A MONTH. IF YOU DON'T KNOW WHAT [redacted] IS GO TAKE A LOOK FOR YOURSELF : [redacted]
THESE ARE GOOD FOR DEPOSITING CERB / DOING EMT'S / OR LINKING TO PAYPAL ACCOUNTS, RECEIVING WIRES OR BANK DEPOSITS. AS A BONUS I WILL INCLUDE HOW TO LOAD IT.

THEY COME IN THIS FORMAT :
==========
- NAME :
- ADDRESS :
- DATE OF BIRTH :
- SIN :
- PHONE :
- DL :
- EMAIL ACCESS:
- LOGIN :
- PASSWORD :
- SECURITY QUESTIONS AND ANSWERS :

===FOR ANY QUESTIONS OR INQUIRY'S DON'T HESITATE TO CONTACT ME ===

Example: Services



Example: Information

▲ △ [redacted] PICKUP IN STORE+BINS ▲ △ ▲

Sold by: GOODPROFILESFORU
Trust rating: High
Feedback score:97
Contact GOODPROFILESFORU
View GOODPROFILESFORU's profile

Auto-delivery

Buy now
99 CAD
74 USD
You are protected by ESCROW

Product Description | Refund Policy | Seller's Feedback

COVID CREATED LOTS OF OPPORTUNITY'S FOR US SCAMMERS. PEOPLE ARE SCARED TO GO IN THE STORES WHICH HAS FLOODED ONLINED ORDERS FOR CURBSIDE PICKUP! I WILL SHOW YOU GUYS HOW TO KILL [redacted] INSTORE PICKUPS YOU DON'T EVEN NEED ID'S :)
EVERYTHING YOU NEED COULD BE FOUND HERE ON CANADA HQ

CARDING 101: BYPASS VBV & MSC

Sold by: stashthecash
Trust rating: High
Feedback score:95
Contact stashthecash
View stashthecash's profile

Buy now
39 CAD
31 USD
You are protected by ESCROW

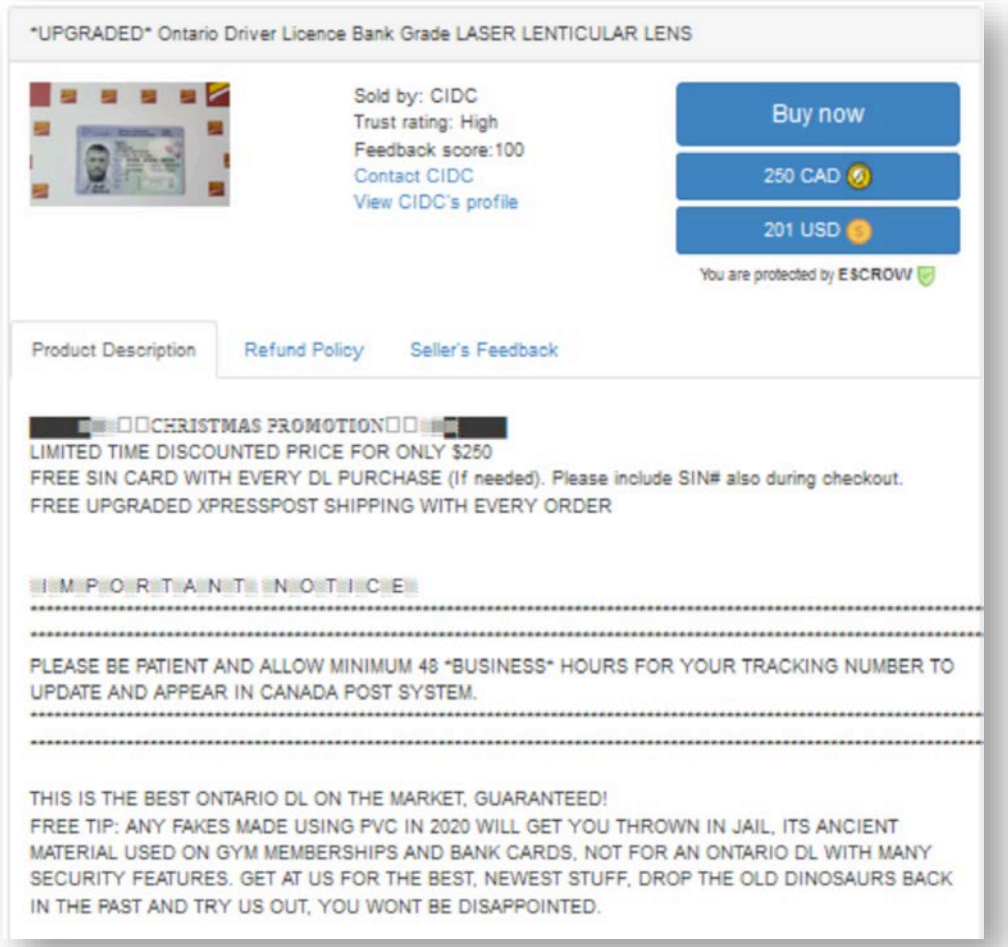
Product Description | Refund Policy | Seller's Feedback

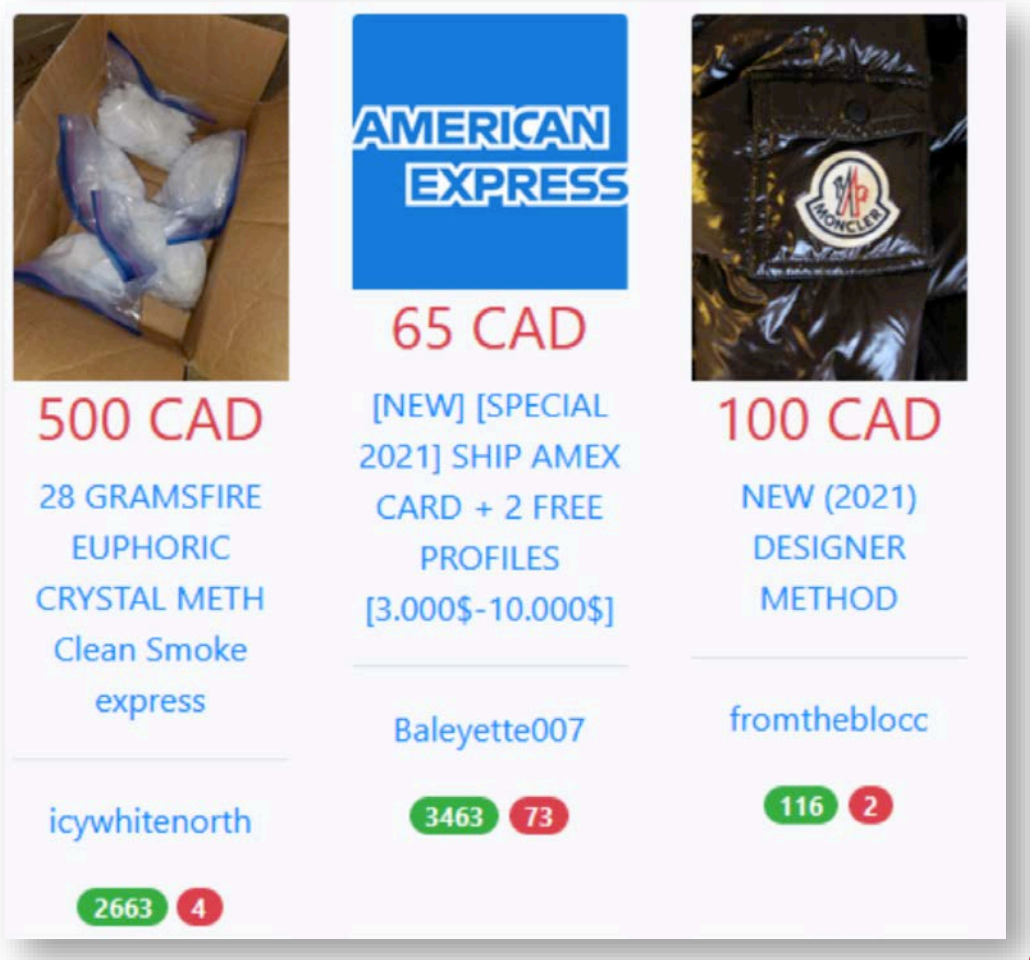
LEARN HOW TO BYPASS VERIFIED BY VISA AND MASTERCARD SECURE CODE AT THE CHECKOUT WHEN CARDING ONLINE WITH THESE TACTICS.

CONTACT IF YOU HAVE ANY QUESTIONS.
RESALE WILL RESULT IN PERMANENT BLACKLIST.

#STASHTHECASH

Example: Physical Goods

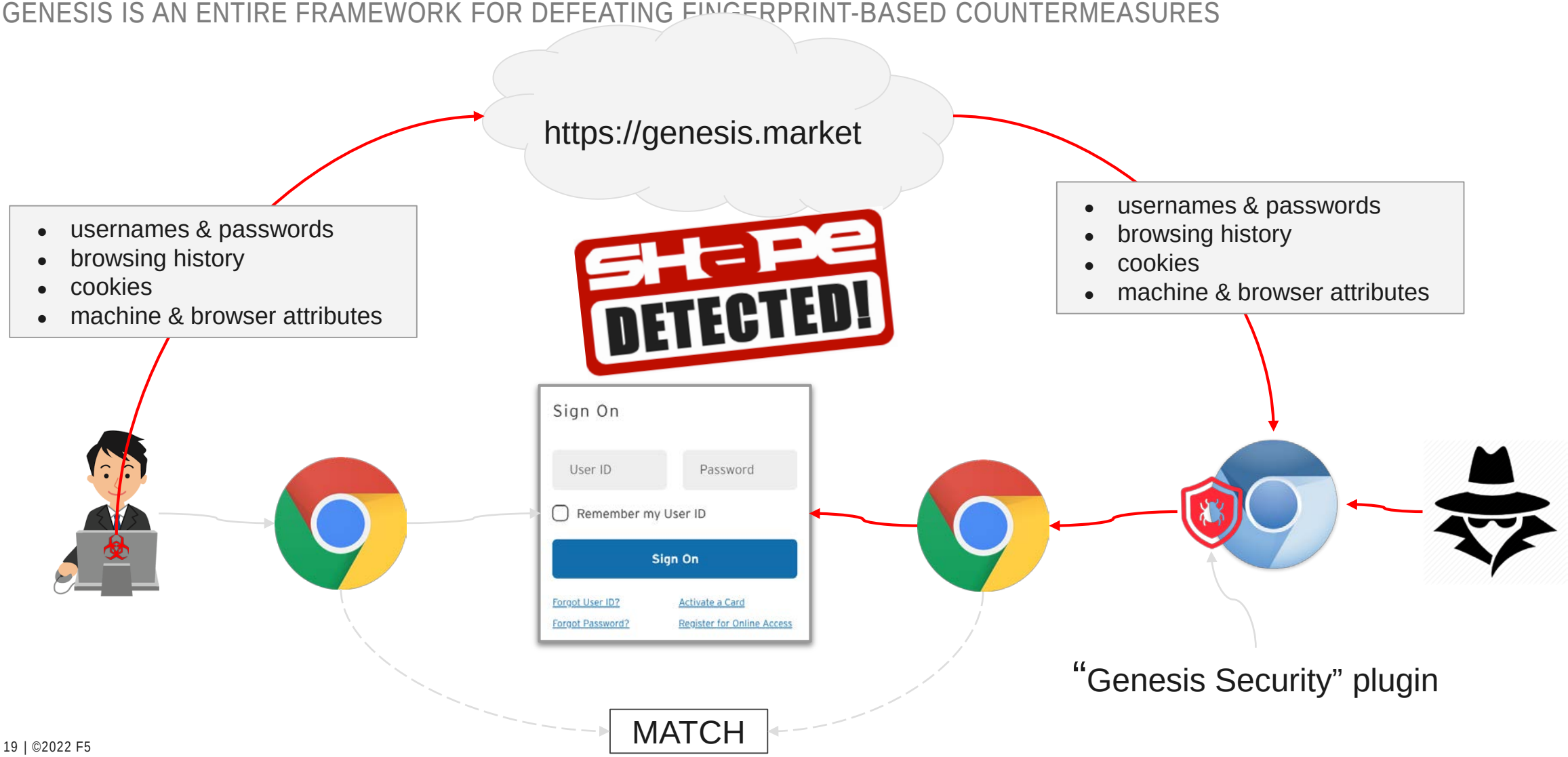




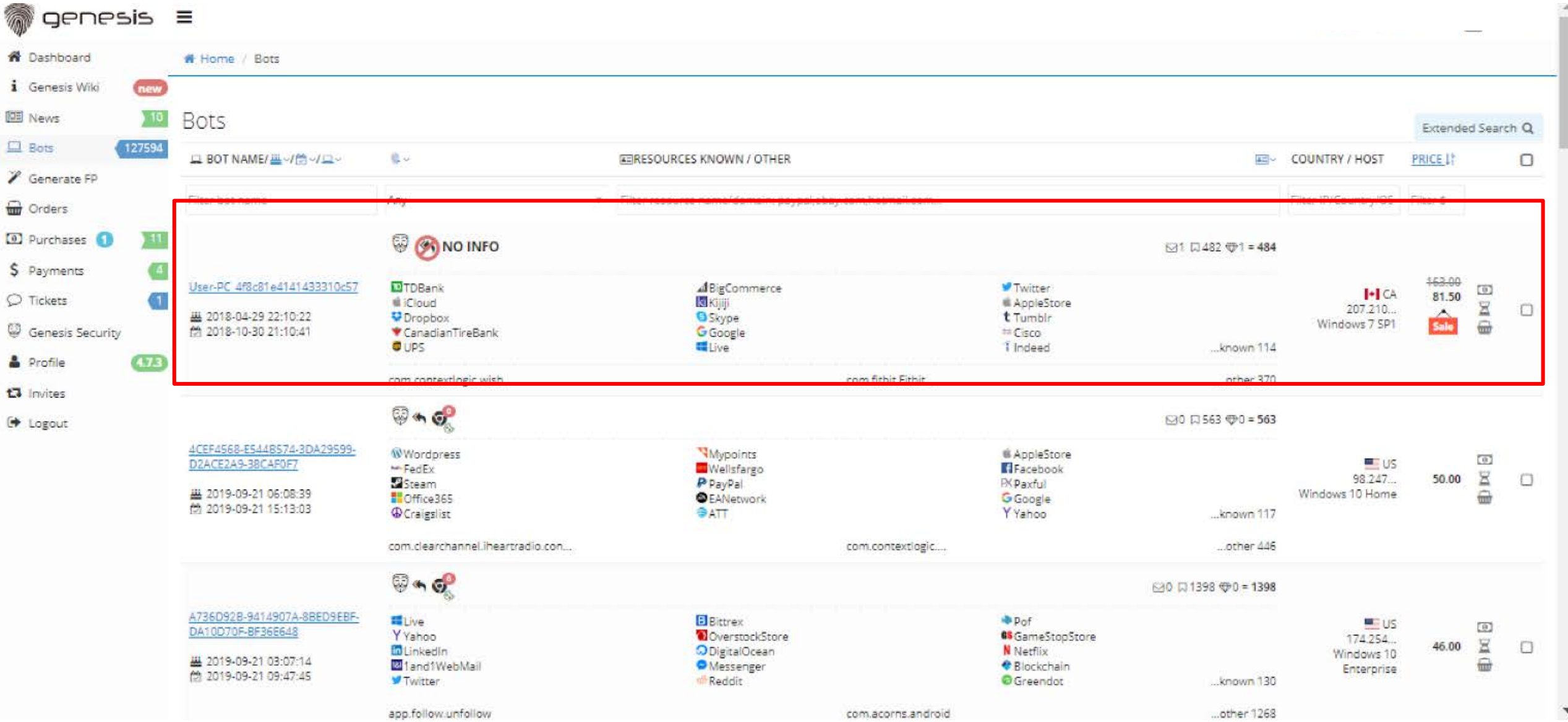
Genesis Crimeware

Genesis: the big picture

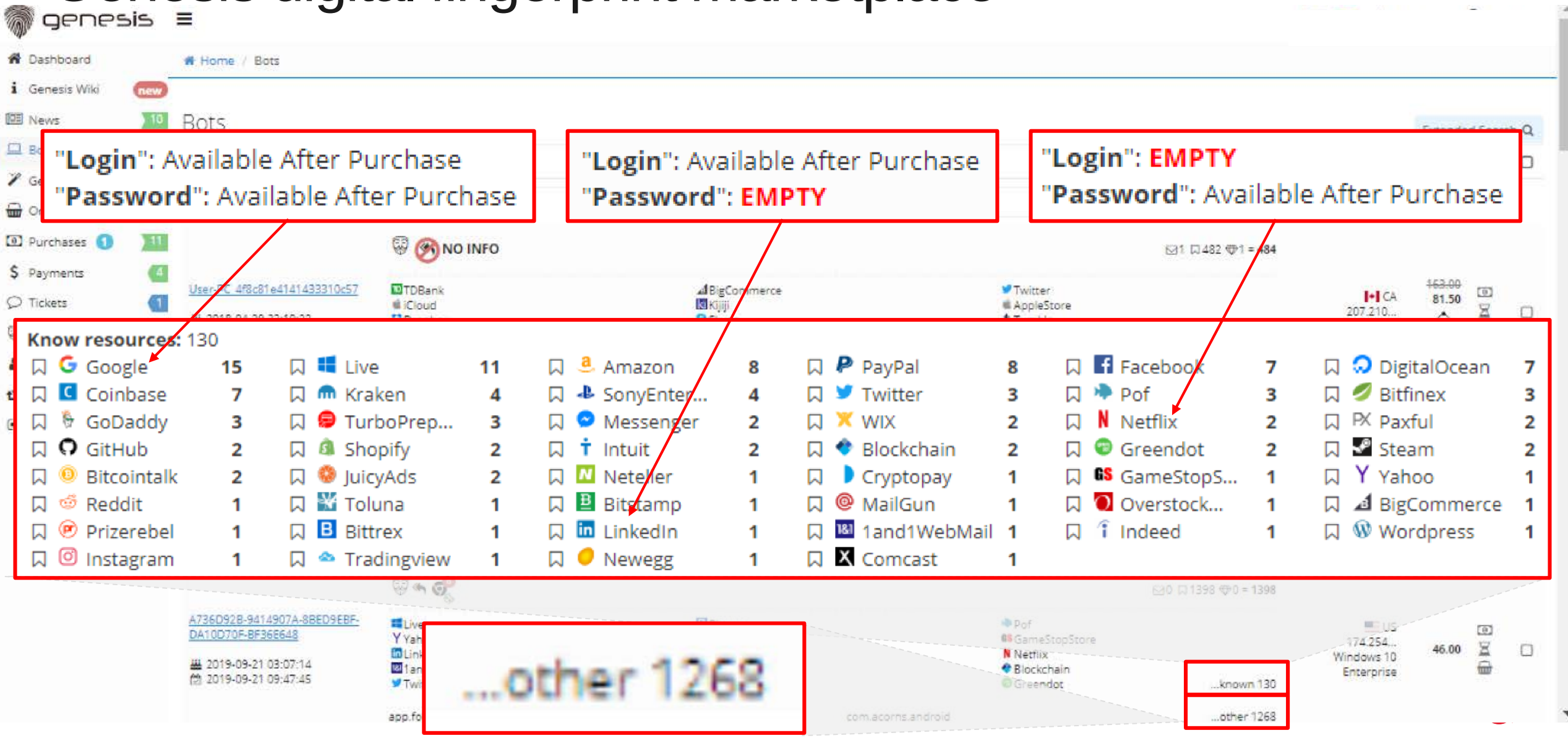
GENESIS IS AN ENTIRE FRAMEWORK FOR DEFEATING FINGERPRINT-BASED COUNTERMEASURES



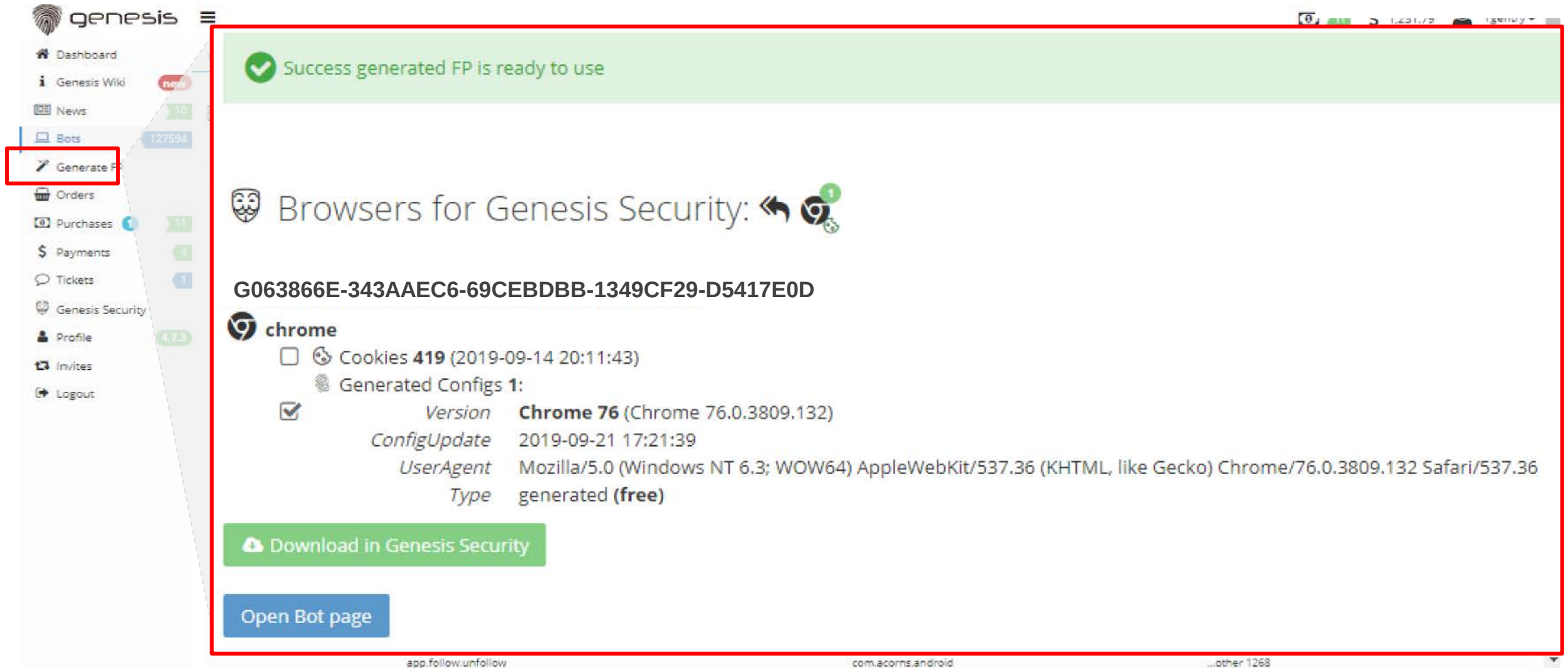
Genesis digital fingerprint marketplace



Genesis digital fingerprint marketplace



Genesis digital fingerprint marketplace



Genesis developers' loyalty is clear

> The Store **does not use or sell** any products connected with **CIS**-countries' web-resources.

Dark Web Stats

Stats: Accounts for sale

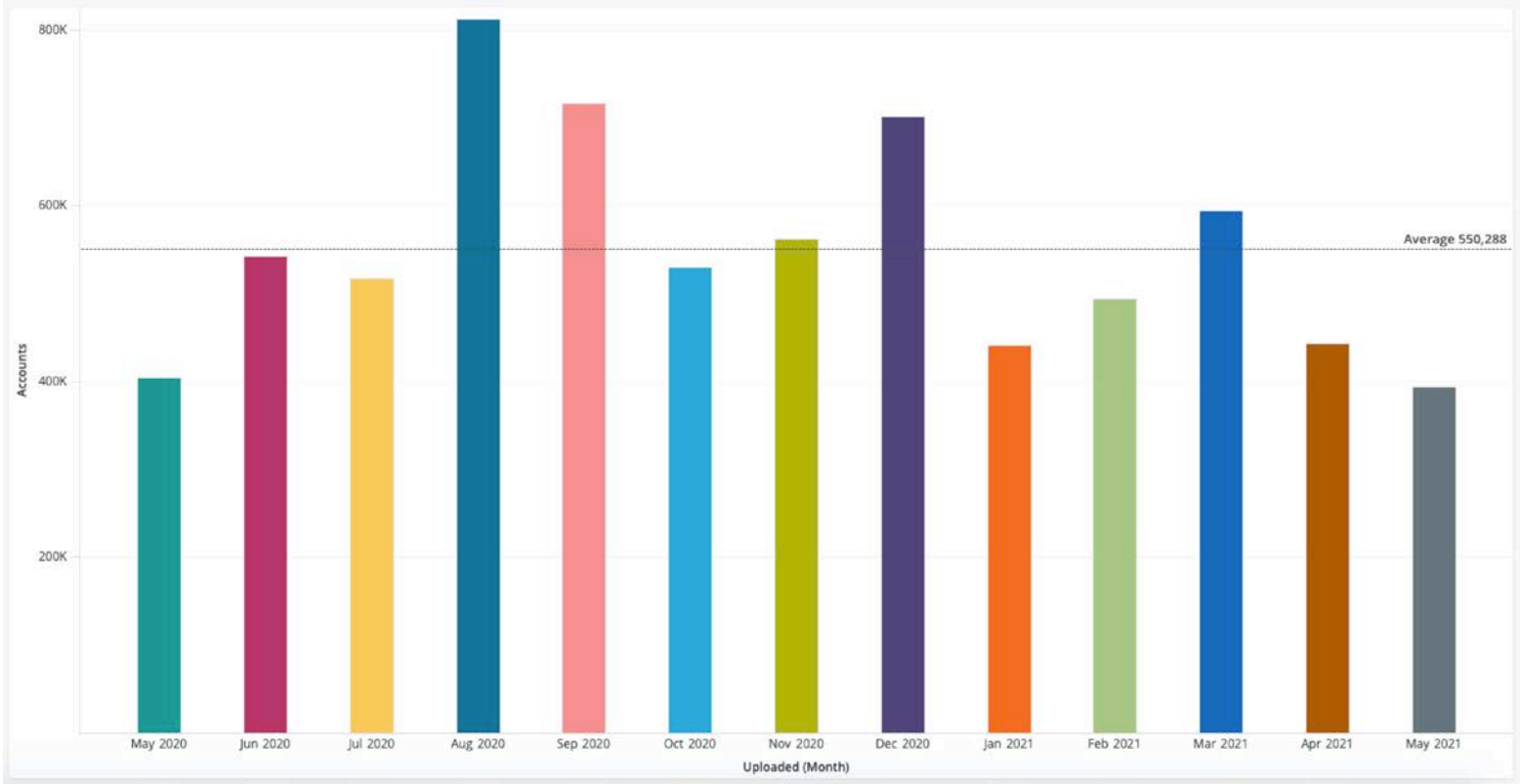
TAKEN FROM ONE DARK WEB SITE

720
Unique Businesses

7.2M+
Accounts

$20M+ in Account Costs

Accounts For Sale
May 2020 – May 2021



Stats: Top 40 Businesses with Accounts for Sale

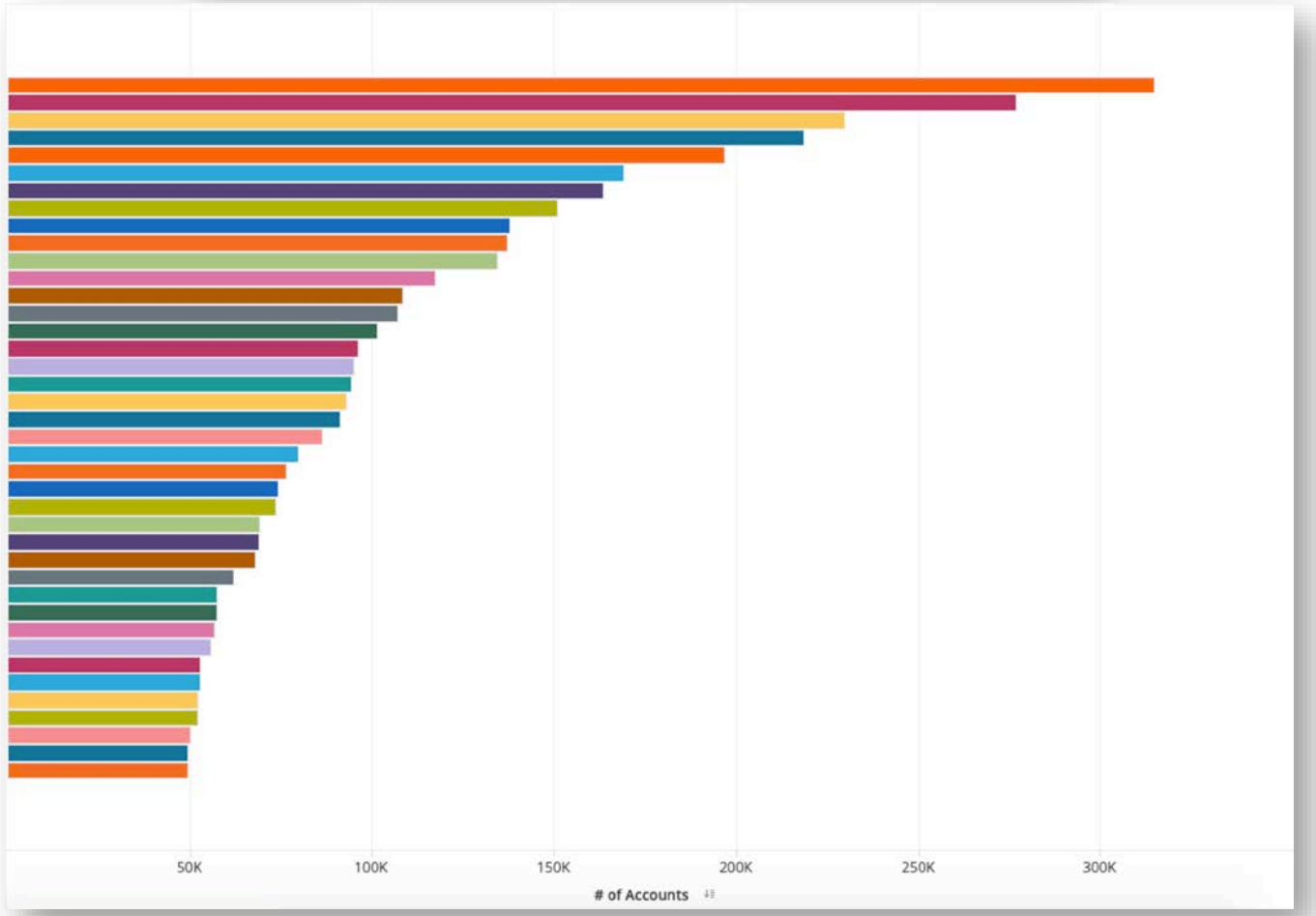
TAKEN FROM ONE DARK WEB SITE FOCUSED

#1 Spot
Over 300K+

Top 2-4
Over 200K+

Next 11
Over 100K+

Top 40 Businesses By Accounts
May 2020 – Mar 2021



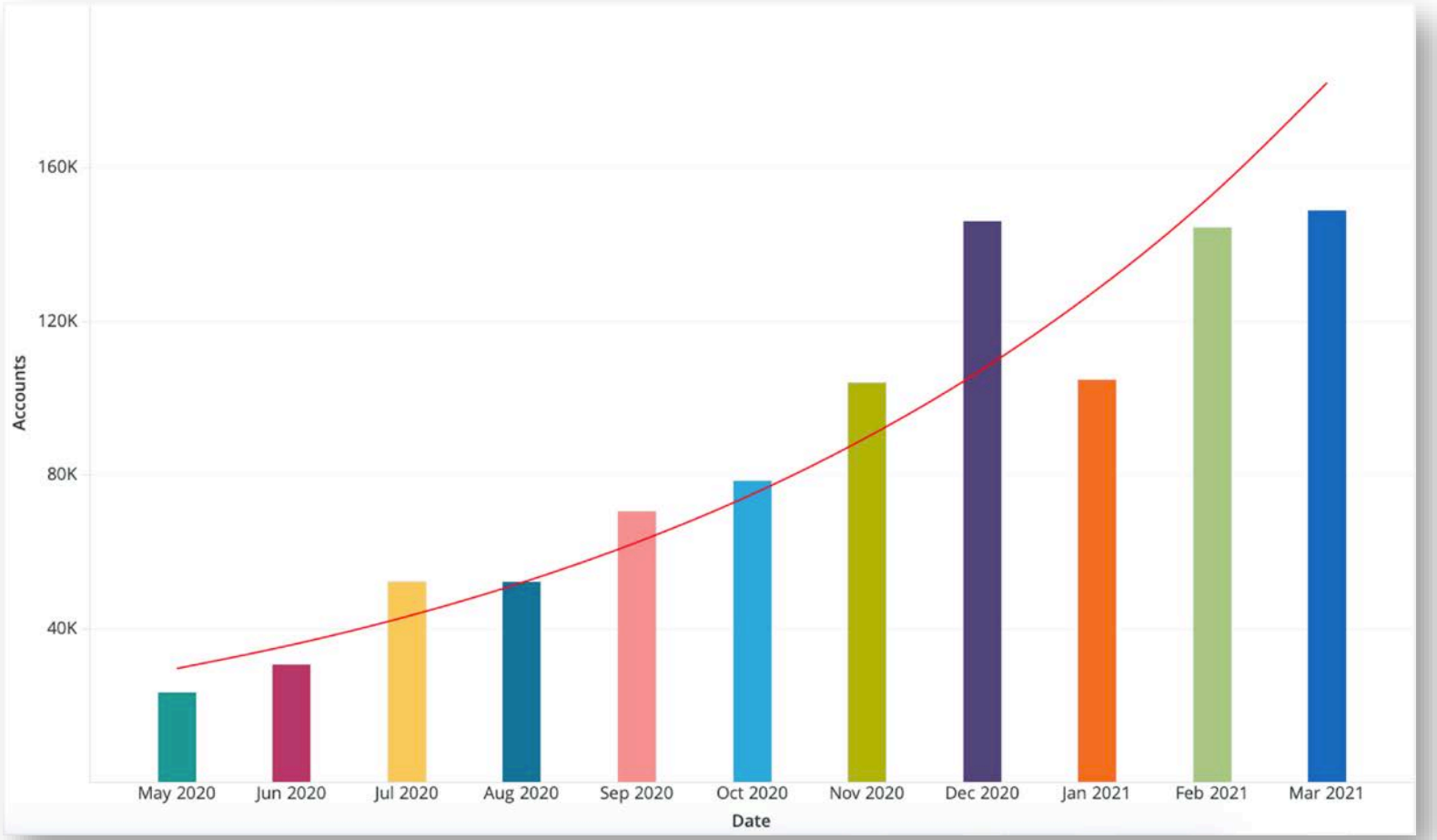
Stats: Mailbox ATO

DATA FROM ONE DARK WEB SITE

149K+ Accounts in Feb

600% Increase from May -> Mar

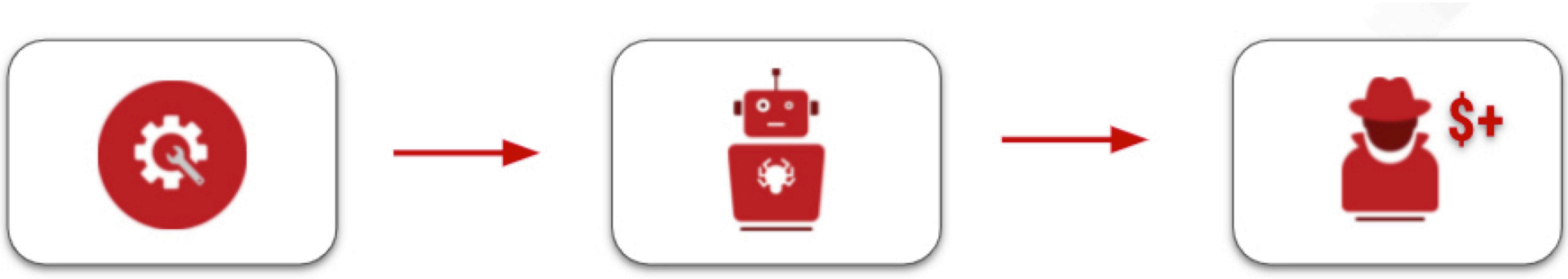
Mail ATO Accounts For Sale
May 2020 – Mar 2021



Account Take Over (ATO) and Attack Tools Discussion

Credential Stuffing

AUTOMATED INJECTION OF USERNAME/PASSWORD PAIRS IN ORDER TO FRAUDULENTLY GAIN ACCESS TO USER ACCOUNTS



Tools/Resources

- Acquire user/pass lists (combo list)
- Proxies
- Captcha Bypass
- Server resources

Account Takeover

- Using cloud resources or credential stuffing services perform attack
- Expect 0-2% success rate depending on quality of the list

Monetization

- Determine how to best profit from accounts
- Exchange points for rewards which can be easily sold eg. Gift Cards
- Use accounts to purchase/pickup items
- Sell accounts on the dark web

Tools and Resources

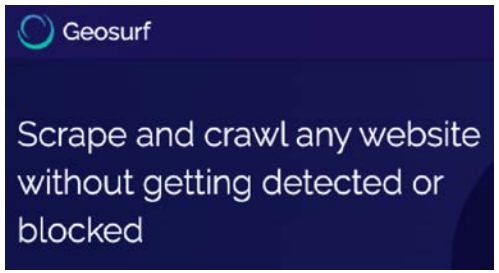
Combo List

- TXT or CSV files containing lists of Usernames/Emails and Passwords
- Many are from past data leaks other can take portions of those lists and make modifications

  Example: Password01 -> Password02

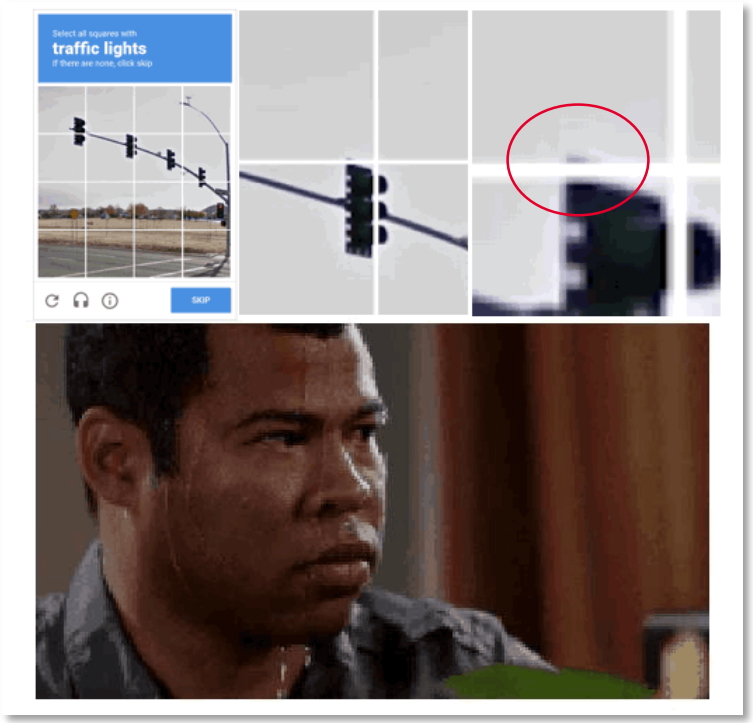
Proxy Lists

- …and the lie begins
- Attackers would prefer to remain hidden and come from multiple sources to prevent easy IP blocking
- There are hundreds of sources to get high quality proxies which can come from any country and even residential IP space



Tools and Resources – Captcha

Customer Experience



Customer Friction

Attacker Solution

Credential Stuffing

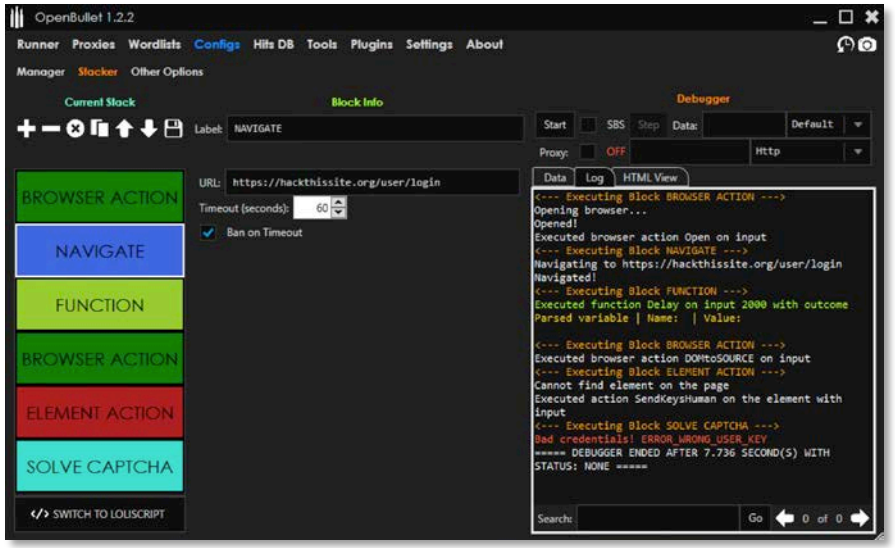
CURL / Bash Scripts

- Bypass browser directly POST to login endpoint
  - Low resources and simple
  - Extra effort to customize scripts and bypass captcha

```
curl 'https://www.hackthissite.org/user/login' \
  -H 'authority: www.hackthissite.org' \
  -H 'pragma: no-cache' \
  -H 'cache-control: no-cache' \
  -H 'sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92"' \
  -H 'sec-ch-ua-mobile: ?0' \
  -H 'upgrade-insecure-requests: 1' \
  -H 'origin: https://www.hackthissite.org' \
  -H 'content-type: application/x-www-form-urlencoded' \
  -H 'user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36' \
  -H 'accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' \
  -H 'sec-fetch-site: same-origin' \
  -H 'sec-fetch-mode: navigate' \
  -H 'sec-fetch-user: ?1' \
  -H 'sec-fetch-dest: document' \
  -H 'referer: https://www.hackthissite.org/user/login' \
  -H 'accept-language: en-US,en;q=0.9' \
  -H 'cookie: HackThisSite=lpgn46vm7ahhq83av1fkfr89i3' \
  --data-raw 'username=test&password=test' \
  --compressed
```

Attack toolkit – Openbullet

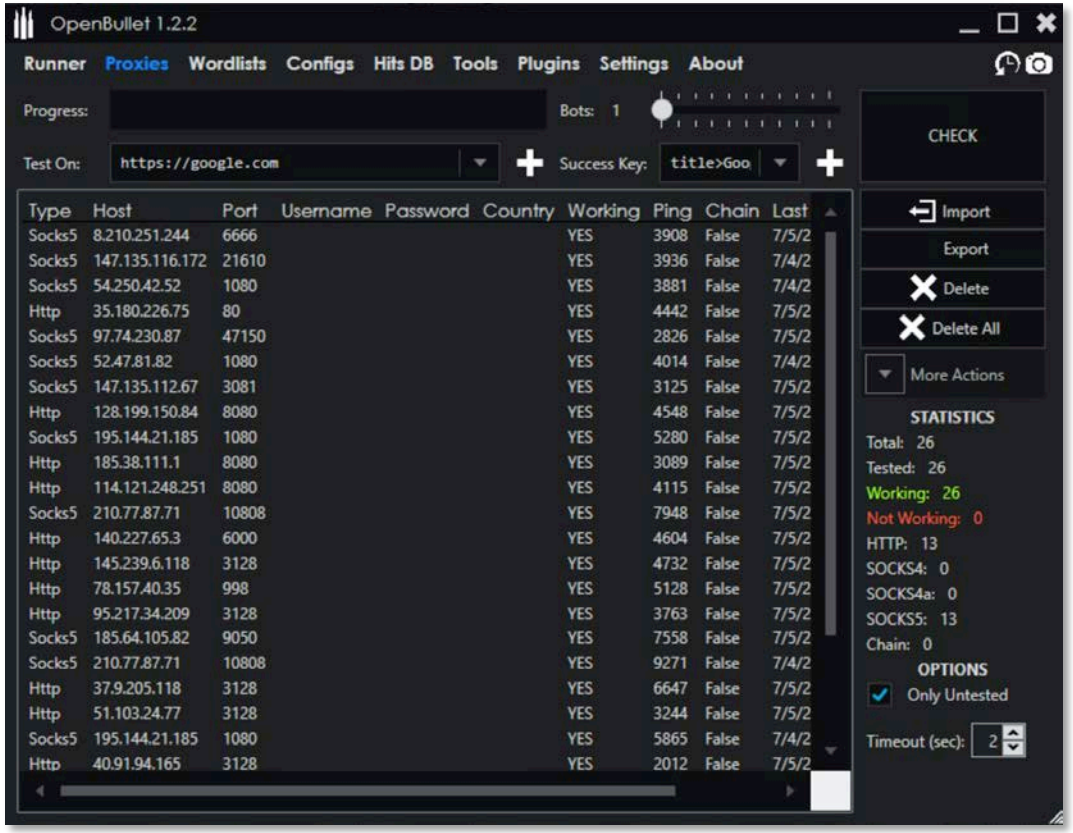
- Easy to configure everything from proxies to captcha bypass
- Can control Browsers or POST directly



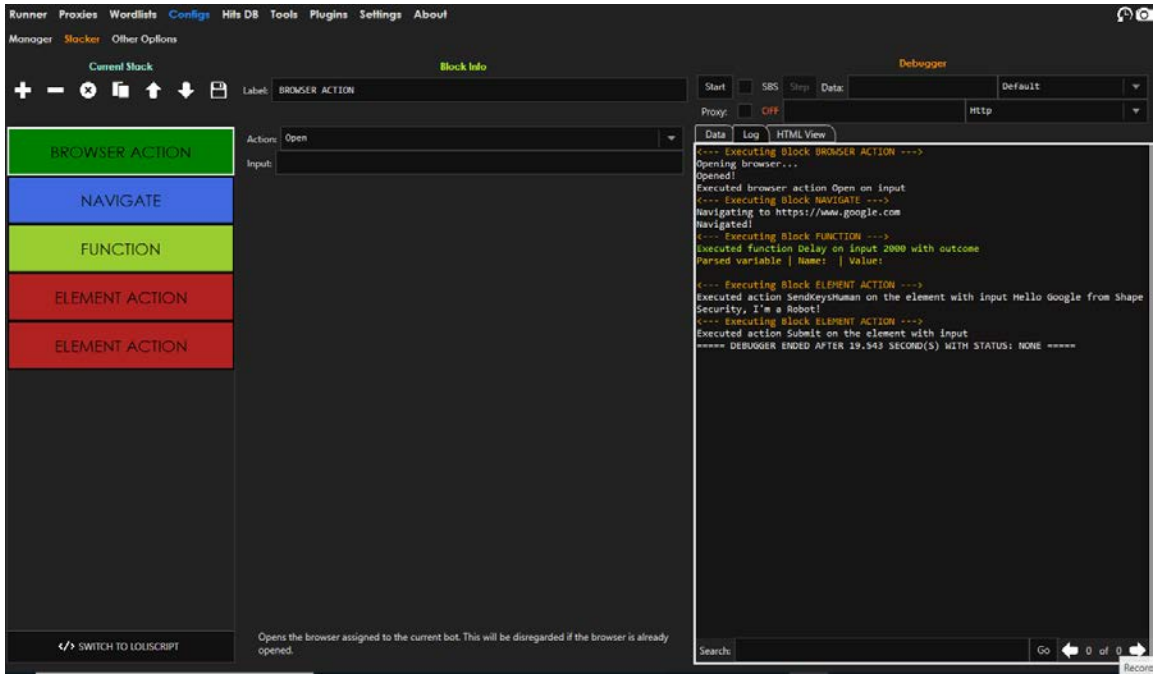
Openbullet

REMOTE BROWER CONTROL WITH A GUI

Integrated Proxy Checker



Openbullet Demo



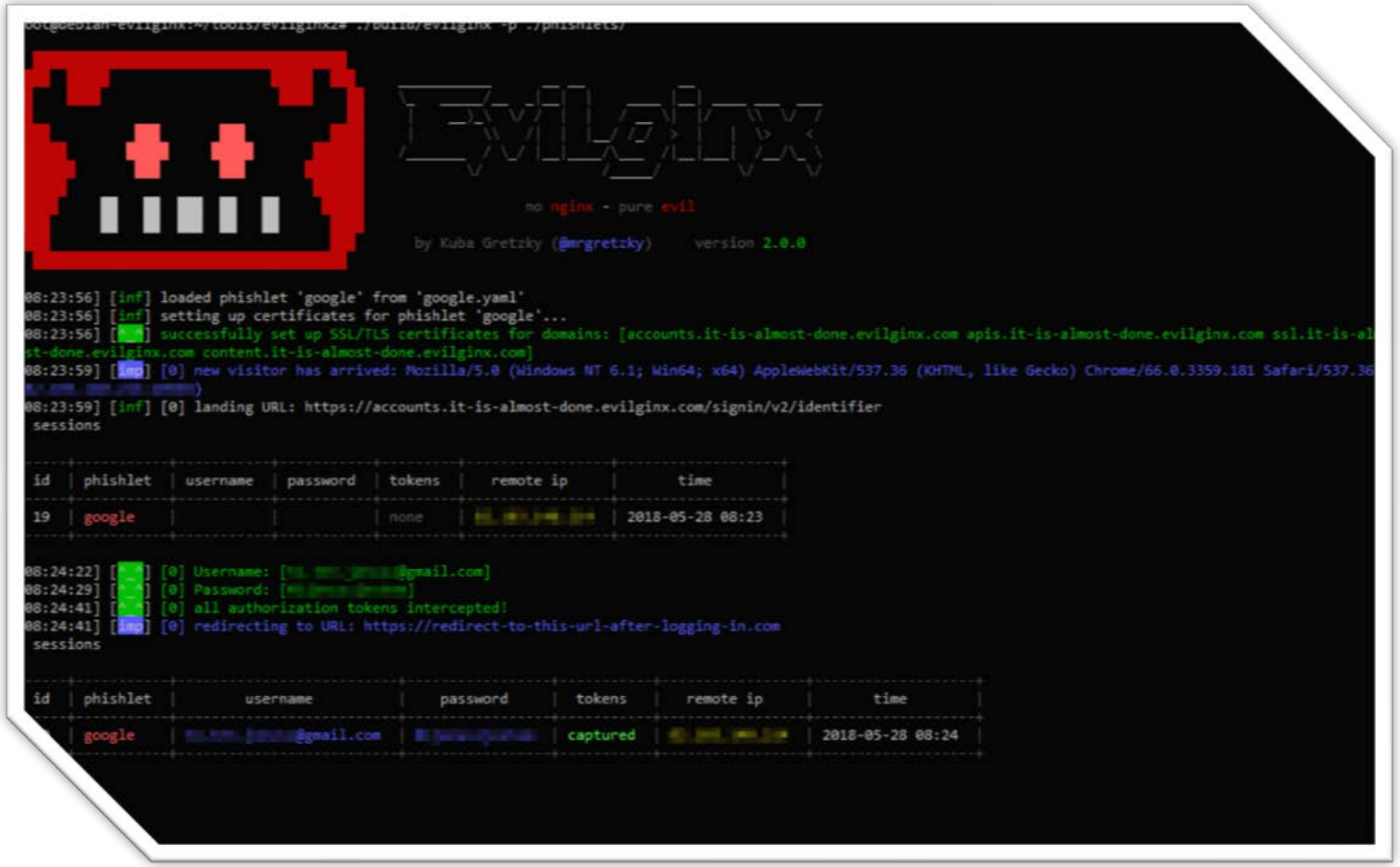
Example: Credential Stuffing Service

ID	NAME	DESCRIPTION	IS CAPTCHA
1652	[redacted]	Check Login, Get Name, Get Type, Get Sub Type, Get Number, Get Sub Number, Get Status Account	Google reCaptcha

#	PLAN NAME	SHORT NAME	LIMIT CHECK	PAYMENT METHOD	TIME	PRICE
1	gold 5 Threads	G30	UNLIMITED	BTC BCH ETH LTC WMZ PM	30 Days	20 USD
2	gold 5 Threads	G60	UNLIMITED	BTC BCH ETH LTC WMZ PM	60 Days	40 USD
3	gold 5 Threads	G90	UNLIMITED	BTC BCH ETH LTC WMZ PM	90 Days	60 USD
4	gold 10 Threads	G30T10	UNLIMITED	BTC BCH ETH LTC WMZ PM	30 Days	40 USD
5	gold 10 Threads	G60T10	UNLIMITED	BTC BCH ETH LTC WMZ PM	60 Days	80 USD
6	gold 10 Threads	G90T10	UNLIMITED	BTC BCH ETH LTC WMZ PM	90 Days	120 USD

Phishing with Evilginx (evil-jinx)

- Automates the process of setting up a man in the middle phishing proxy
- People can be easily fooled as the application proxies the login towards the real site so victim see their real data

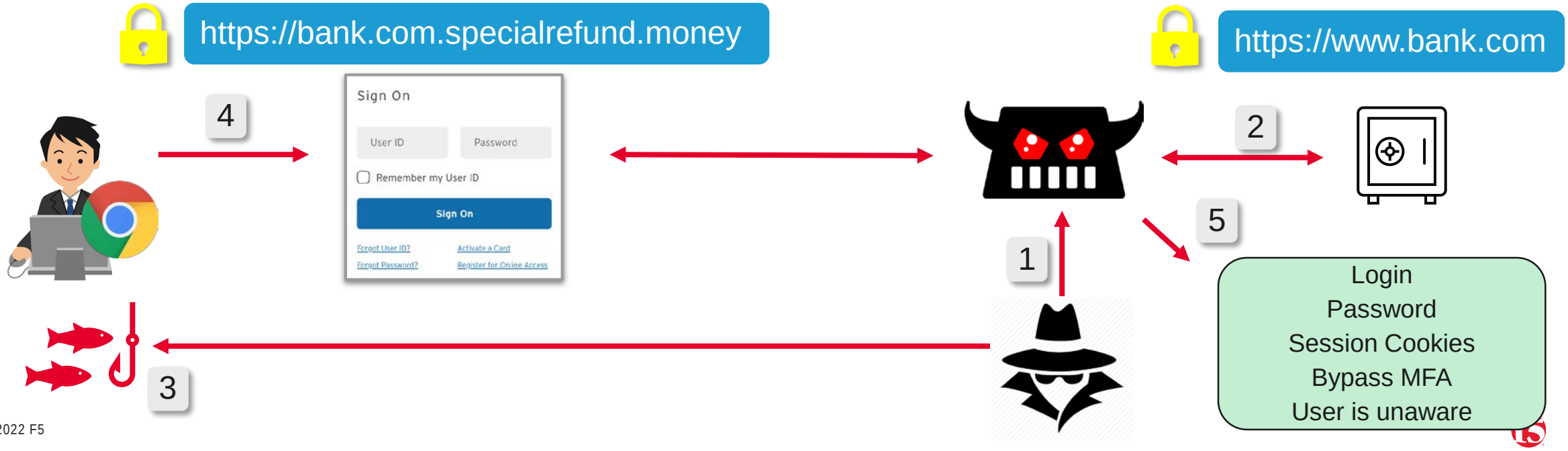


Evilginx 2: Man-in-the-middle attack framework

A FEW CLICKS TO SITTING IN THE MIDDLE

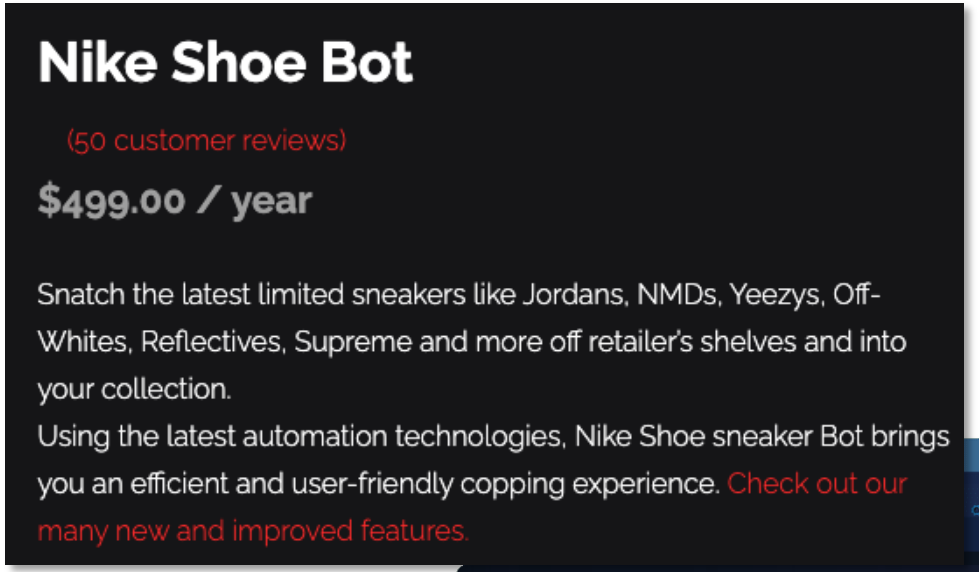
- Attacker convinces victim to use phishing link
- Victim sees the SSL lock icon
- Victim sees their real site data

- Create Evilginx2 Phishlet
- Auto retrieves LetsEncrypt SSL/TLS Certs
- Creates Phishing link DNS entries



Retail Purchase Bots

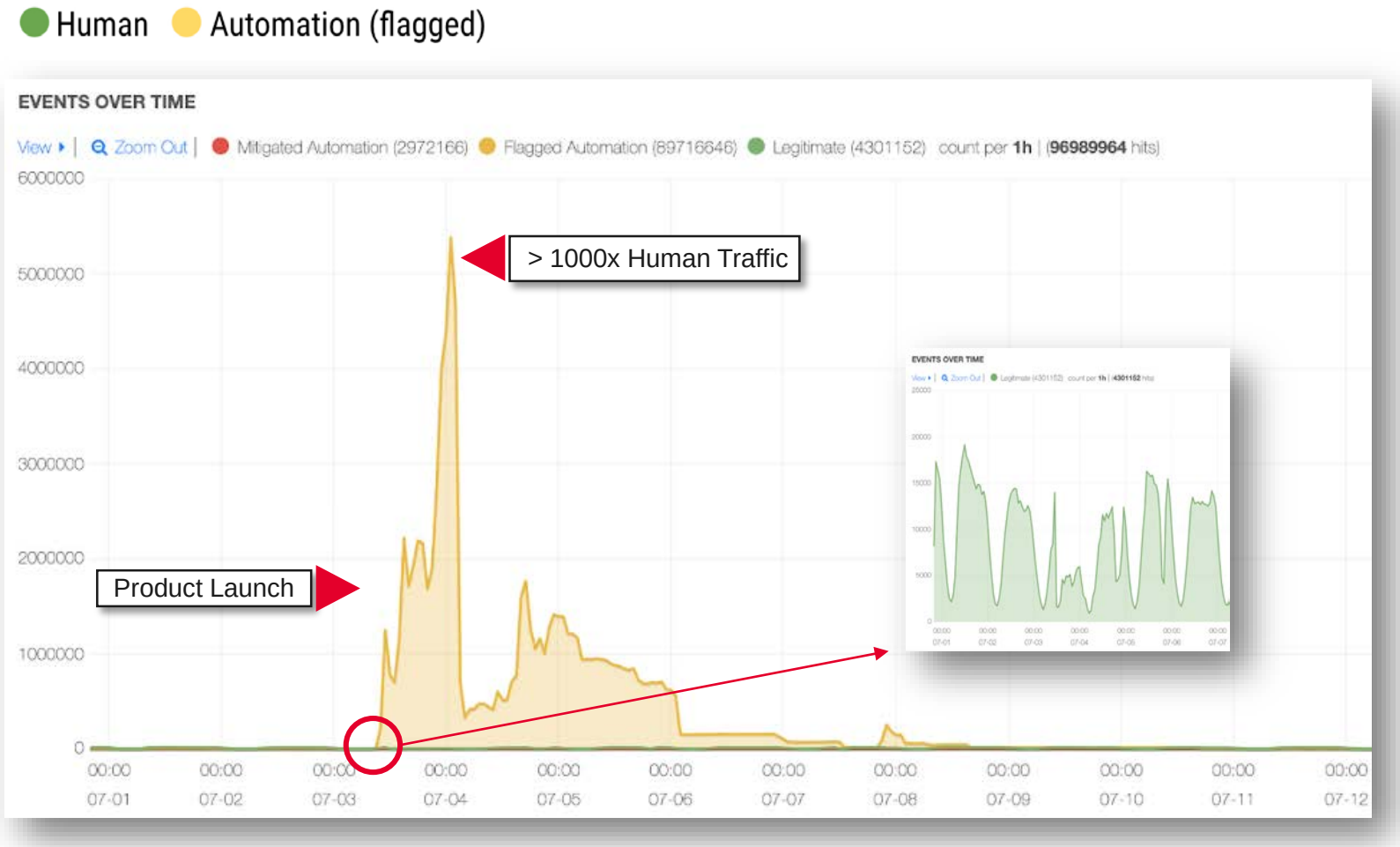
- Wondering why you can't get that PS5, RTX 3090, or the latest set of kicks?
- Bots specifically design to constantly monitor for stock and then quickly add and checkout items before you ever had a chance



Example: Purchase Bots in Action

ARE YOU JUST PAYING RESOURCES FOR BOTS?

- Highly desirable product launch
- Bots were active before product went live
- Bots attacked customer “Add to Cart” with millions of requests
- > 1000x Human Traffic



Accessing it safely

Safety First

1. • DO NOT USE YOUR PERSONAL SYSTEM DIRECTLY
2. • DO NOT USE YOUR CORPORATE SYSTEM DIRECTLY
3. • Be careful which links you follow
   • There is no honor among thieves
4. • Follow your business internet access policies
5. • Don't use your corporate or personal email when registering
   • Create a new email via protonmail.com or similar

Experience

"Experience is something you get just after you needed it"

How to assess potential exposure

Use Google-Fu Search Skills to search public forums and shops

- The below query pasted into the search box can potentially turn up results
- `(companyname.com | companyname) site:https://www.reddit.com/r/shoppingbay OR site:https://www.reddit.com/r/shopping OR site:nulled.to OR site:cracked.to OR site:shoppy.gg`
- Search Ebay / AliExpress and similar sites

Are customer taking the bait of Phishing Sites

- When accounts have value typically there will be a those trying to steal credentials via phishing
- Two free resources are Phishtank.com and Phishstats.info (Use caution when following any Phishing Link)

Steady yourself and venture into the Dark Web

- Starting with resources on the follow page and venture slowly from there
- You may not find anything immediately; some accounts or methods never make it to dark markets for sale
- Follow site instructions regarding bookmarking of main pages. Fake sites consistently pop-up trying to phish other scammer credentials

Access Recommendations

Hoodie + Matrix Background

- Optional Guy Fawkes Mask

Base - Virtualized System

- This can be separate Server or Cloud based solution
- Or local software such as VirtualBox / VMware Workstation

Network Layer

- Dedicated and restricted network segment if possible
- VPN with local Firewall to prevent access to local resources
- TOR Proxy

Browser

- TOR Browser is a secure browser that receives regular updates and includes a TOR Proxy
- Regular browser: Extension such as NO-Script to limit JS execution (some JS may be required)

Starting Resource

Phishing

- PhishTank - https://Phishtank.com
- PhishStats - https://Phishstats.info

Public Forums

- https://shellix.xyz / https://tmart.io
- https://nulled.to
- https://cracked.to
- https://www.reddit.com/r/shoppingbay
- https://disboard.org/search
- Ebay / AliExpress

Dark Markets

- TOR Directory - Dark Fail - https://dark.fail | darkfaillnkf4vf.onion
- Accounts Market - Base69 - https://base69.net
- Credential Stuffing/Credit Card Validation - SRV11- https://srv11.net
- Accounts/Methods/Physical - CanadaHQ - http://canadahq2lo3logs.onion (now requires a deposit before searching)

Protecting your Apps

F5 XC Platform

Multi-layered, highly effective modern app security bringing together the best of f5 application security

Advanced Application Security		WAAP		Integrated Services	
Authentication Intelligence			Web Application Firewall	DNS	Application Traffic Insight
Account Protection (Anti Fraud)	Advanced Bot Defense	Bot Defense	API Security	Load Balancing	AppStack Managed Kubernetes
Client-Side Defense			DDoS Mitigation	Mesh Multi Cloud Infrastructure	Customer Portal

F5 Distributed Cloud (SaaS)

 Multi-Cloud

 On-prem

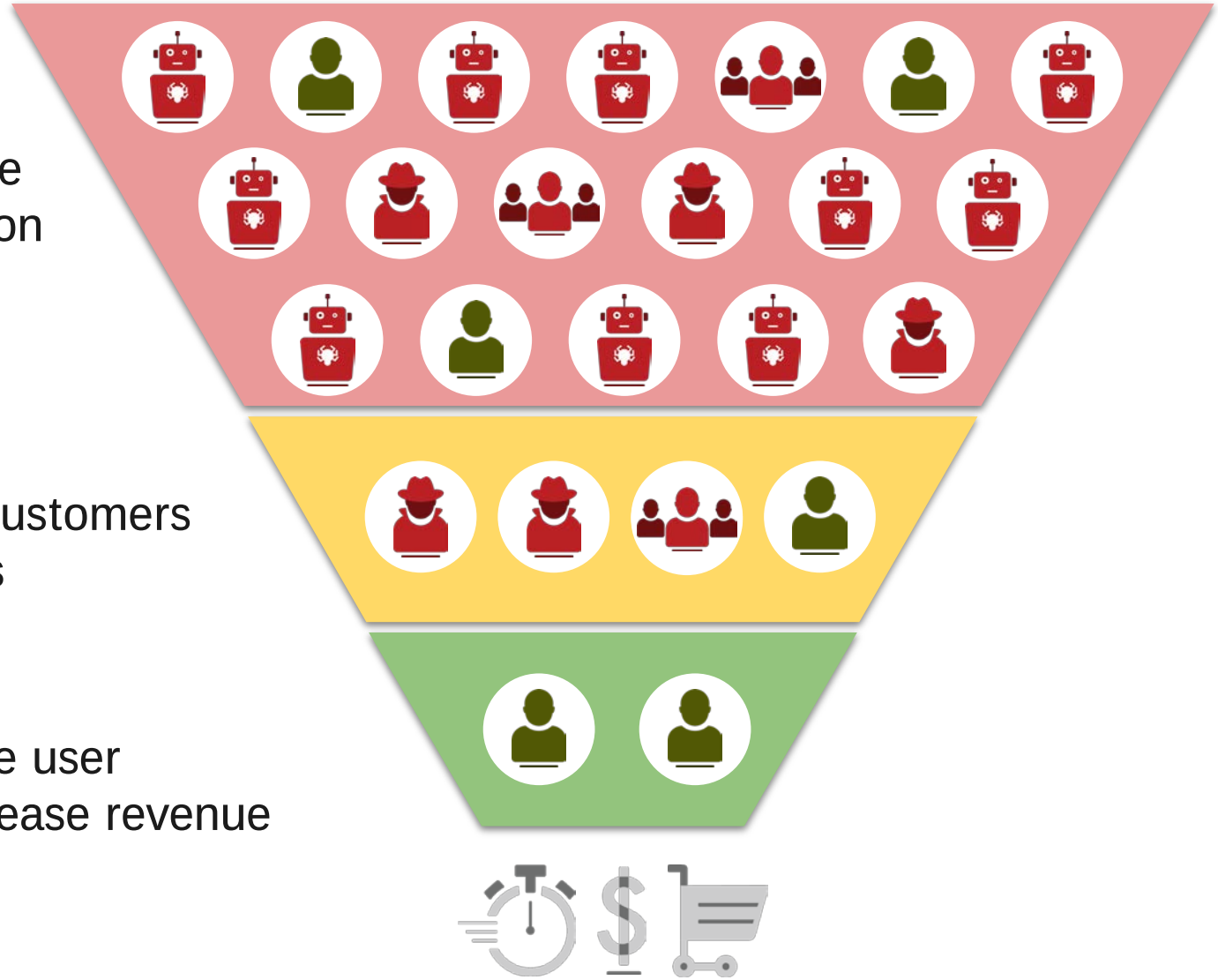
 Edge

The Power of F5 XC – Advanced App Security

FICTION
Identify and mitigate unwanted automation traffic

FRAUD
Differentiate good customers from bad customers

FRICTION
Create a friction free user experience and increase revenue



Bots

Human Clickfarm

Fraudsters and Criminals

Good customers