



**Controlware
Security Day**

22. - 23. September 2022
Congress Park Hanau

controlware

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

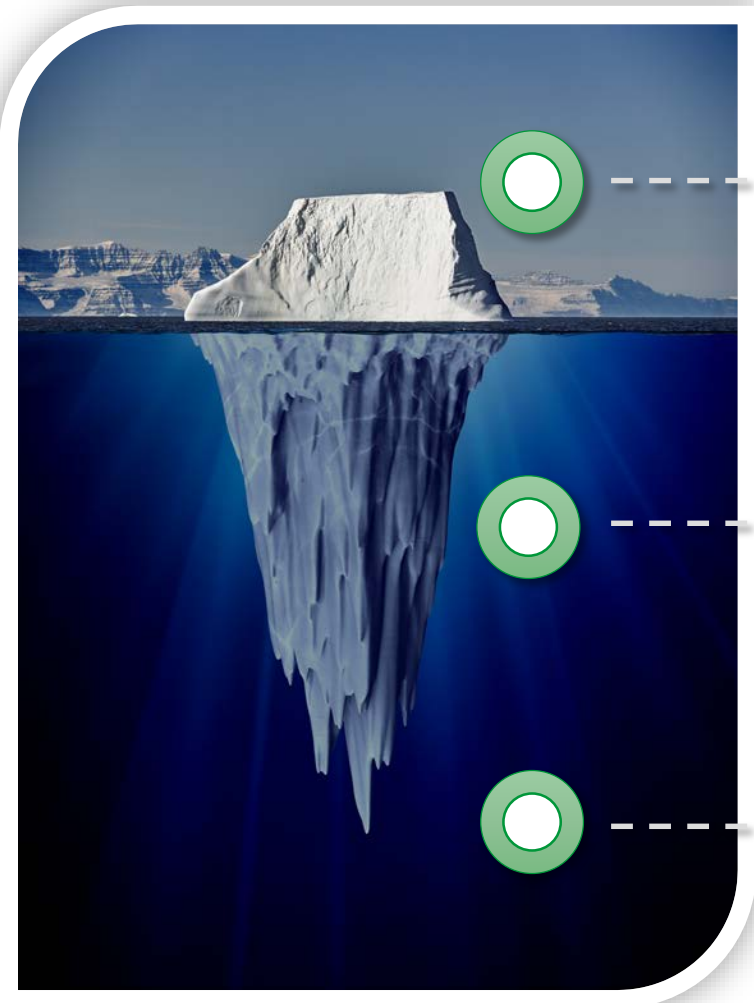
What is the “Dark Web”

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 portrayed as a secret member of the hoodie and Matrix fan club and sometimes with their appreciation for Guy Fawkes masks



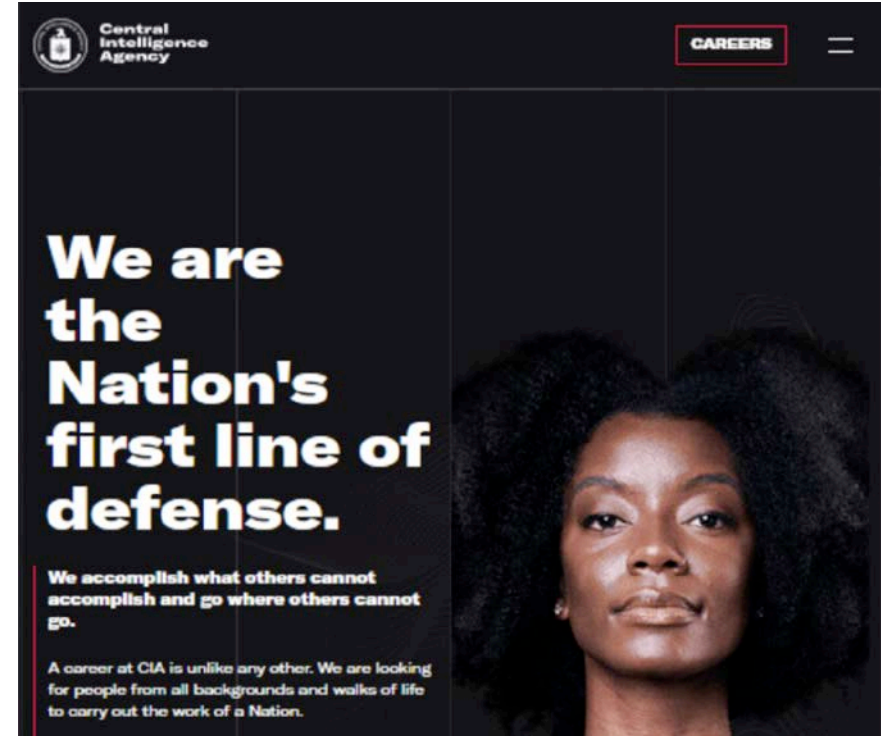
What can you find

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

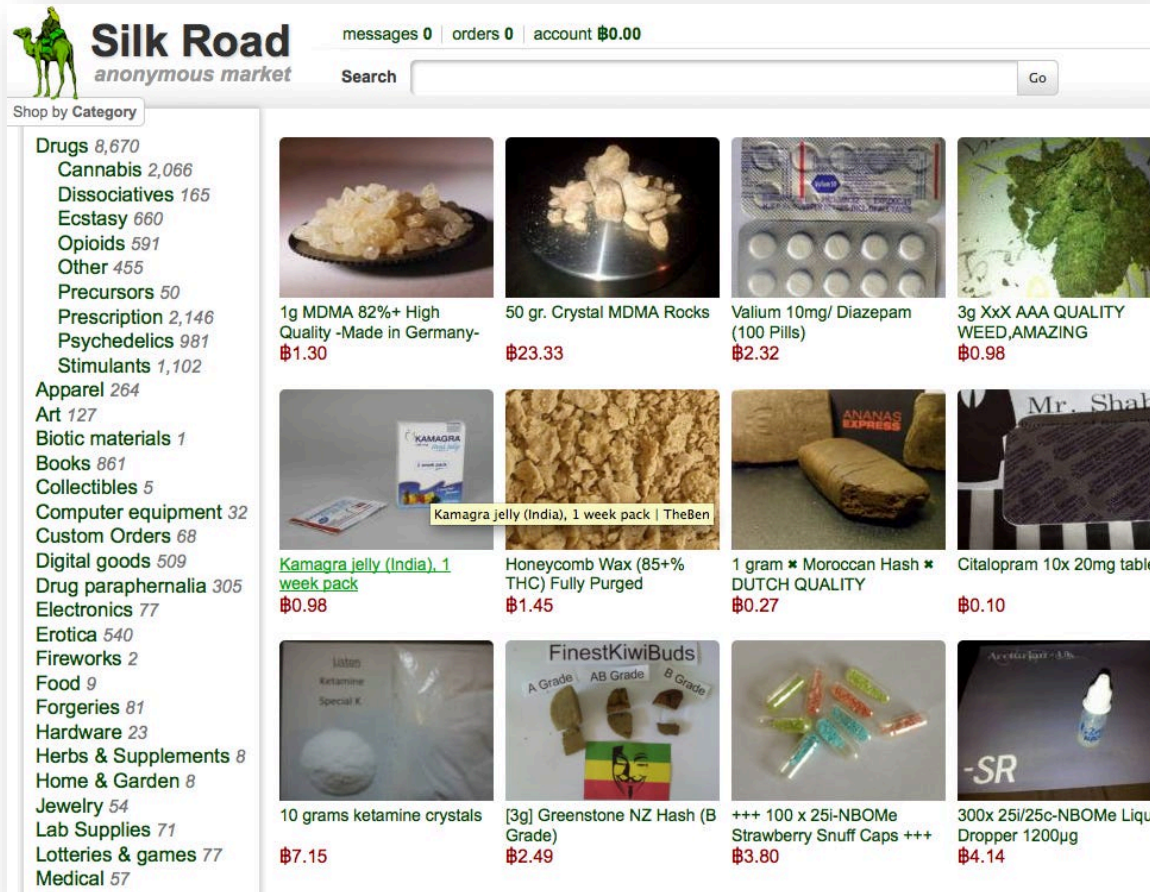
- Reddit r/ShoppingBay
- Forums such as Nulled or Cracked
- Shopsy, Sellix, eBay, AliExpress Stores
- Aggregators, Discord and Telegram channels

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



DOJ Announces Successful Disruption of Compromised Credential Marketplace "SlilPP"

On June 10, 2021, the US Department of Justice (DOJ) announced the successful disruption of the illicit, cybercriminal credential marketplace known as "SlilPP," a specialized shop primarily used to conduct the sales and distribution of compromised credentials.

Figure 1: Tor Portal Page for SlilPP Marketplace



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
NA	101111.00	MARGARET	N/A	N/A MA 02122	N/A	N/A	N/A	N/A	@comcast.net	17 Mar 2021	Bunny	52
NA	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
NA	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
NA	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
NA	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
NA	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
NA	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
NA	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
NA	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
NA	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


Fresh  Premium Lifetime Accounts




Sold by: Pegasus
Trust rating: High
Feedback score:99
[Contact Pegasus](#)
[View Pegasus's profile](#)


[Buy now](#)

6 CAD 

5 USD 

You are protected by ESCROW 

Product Description Refund Policy Seller's Feedback

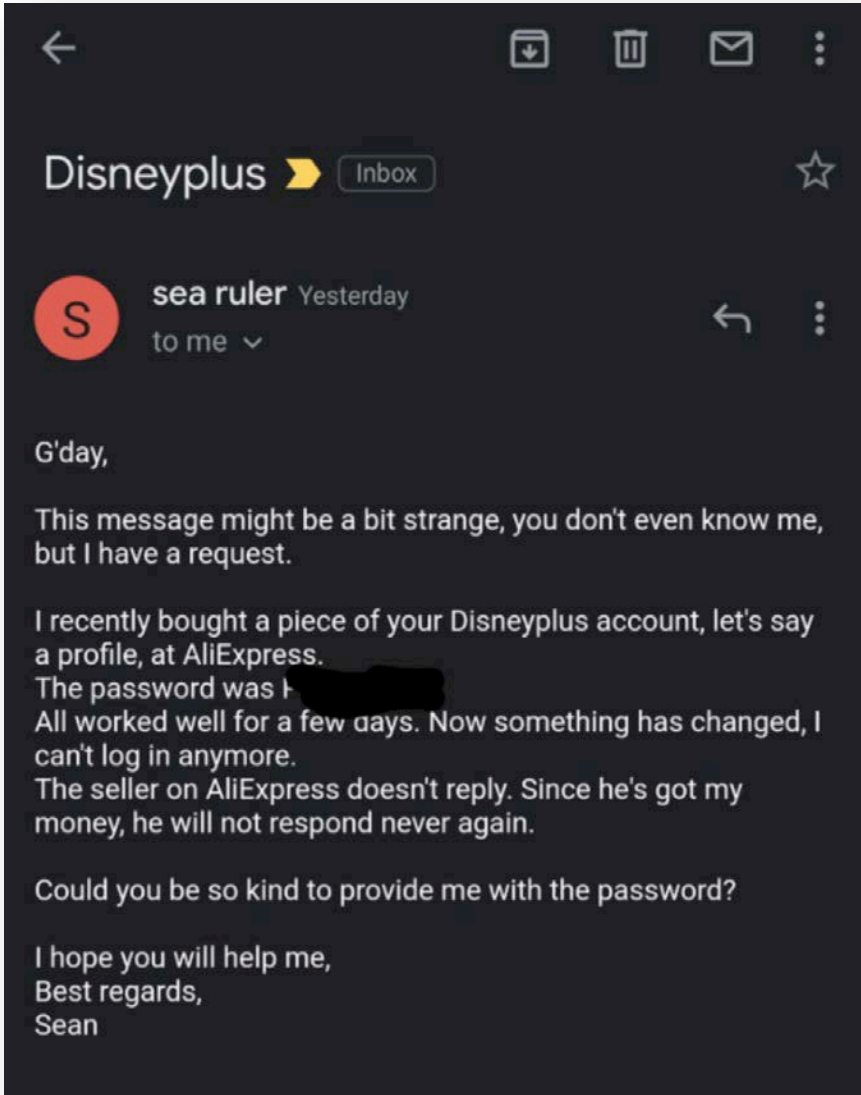
Enjoy Fresh  Premium Lifetime Accounts at low price

If you are not in USA you need to use a VPN set to USA in order to use these accounts.
You can get cheap VPN accounts in my shop.

I replace if it stops working

You will receive the account in this format
Email
Password


Example: Help please...



Example: Financial

Bank

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 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-Transfers
Mobile Deposit Ready for

How to ship a 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 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

ACCOUNT DROPS + HOW TO LOAD***



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

Buy now

70 CAD

56 USD

You are protected by ESCROW

Product Description Refund Policy Seller's Feedback

THESE ARE VERIFIED DROPS CREATED BY MYSELF! AGED ANYWHERE FROM 1 WEEK TO A MONTH. IF YOU DONT KNOW WHAT IS GO TAKE A LOOK FOR YOURSELF :

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 DONT HESITATE TO CONTACT ME ===

Example: Services

INFO77

BEST SERVICE SEARCH SSN & DOB

- We are No. 1 in finding someone's SSN, DOB in the USA
- We succeed over +1000 cases, helping many people confirm successful information for big companies: Amazon, Ebay, Paypal, v.v.
- We work directly on the real information system from the US government, our information is genuine and we guarantee 99.99% accuracy

Future.

Future's Refund Service

Our goal is to provide top quality service to each and every customer. Don't pay a full price when you can save up to 80% of your money.

BUY NOW

PLAN FOR CARD CHECKER UNLIMITED CHECK

Read Me !

"SRV BALANCE" is not used for package conversion and upgrade. "SRV BALANCE" is for Card Checker only. (If you want to use Account Checker, see the table above. Also want to use both Checkers, see the last table)

#	PLAN NAME	SHORT NAME	LIMIT CHECK	PAYMENT METHOD	TIME	PRICE	ACTION
0	Pay As You Go 5 Threads	PAYG	YOUR BALANCE	BTC BCH ETH LTC WMZ PM	Lifetime	Min: 10 USD	ADD MONEY NOW
1	diamond 5 Threads	D30	UNLIMITED	BTC BCH ETH LTC WMZ PM	30 Days	70 USD	UPGRADE NOW
2	diamond 5 Threads	D60	UNLIMITED	BTC BCH ETH LTC WMZ PM	60 Days	140 USD	UPGRADE NOW
3	diamond 5 Threads	D90	UNLIMITED	BTC BCH ETH LTC WMZ PM	90 Days	210 USD	UPGRADE NOW

Process.

how does this work

1 Contact Us

We'll provide you with all information needed before purchasing.

2 Receive your package

Depending on the store, either take sign your package or don't sign it at all.

3 Contact us back

Fill out our form and we will get to work.

4 Pay us our cut

Returning customers receive discounts.

Terms of service


1. My current rate is 10% for each order. Orders below \$300 have fixed fee of \$30.
2. I reserve the right to deny your order.
3. I'm not responsible for what happens after refunding is done.
4. I reserve the right to change this anytime I want.
5. Payment must be sent immediately after refund process is done.
6. By using my service agree to my T.O.S
7. Chargebacks will result informing the store you purchased from. From that point you are facing all consequences.
8. I don't do double dips.
9. I can try a custom store for different fee.

Why choose me?

Our refunding service covers Worldwide stores. We respond the quickest and keep you updated all the time. Being a MPGH's staff member will ensure you top safety. Smallest fees for stores.

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 ONLINE 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


UPGRADED Ontario Driver Licence Bank Grade LASER LENTICULAR LENS




Sold by: CIDC
Trust rating: High
Feedback score: 100
Contact CIDC
View CIDC's profile

Buy now

250 CAD 

201 USD 

You are protected by **E SCROW** 

Product Description | Refund Policy | Seller's Feedback

CHRISTMAS PROMOTION

LIMITED TIME DISCOUNTED PRICE FOR ONLY \$250
FREE SIN CARD WITH EVERY DL PURCHASE (If needed). Please include SIN# also during checkout.
FREE UPGRADED XPRESSPOST SHIPPING WITH EVERY ORDER

IMPORTANT NOTICE

PLEASE BE PATIENT AND ALLOW MINIMUM 48 *BUSINESS* HOURS FOR YOUR TRACKING NUMBER TO UPDATE AND APPEAR IN CANADA POST SYSTEM.

THIS IS THE BEST ONTARIO DL ON THE MARKET, GUARANTEED!
FREE TIP: ANY FAKES MADE USING PVC IN 2020 WILL GET YOU THROWN IN JAIL, ITS ANCIENT MATERIAL USED ON GYM MEMBERSHIPS AND BANK CARDS, NOT FOR AN ONTARIO DL WITH MANY SECURITY FEATURES. GET AT US FOR THE BEST, NEWEST STUFF, DROP THE OLD DINOSAURS BACK IN THE PAST AND TRY US OUT, YOU WONT BE DISAPPOINTED.



500 CAD

28 GRAMS FIRE
EUPHORIC
CRYSTAL METH
Clean Smoke
express

icywhitenorth

2663 4

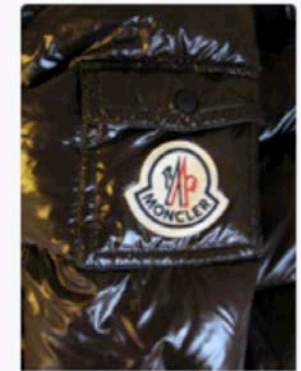


65 CAD

[NEW] [SPECIAL
2021] SHIP AMEX
CARD + 2 FREE
PROFILES
[3.000\$-10.000\$]

Baleyette007

3463 73



100 CAD

NEW (2021)
DESIGNER
METHOD

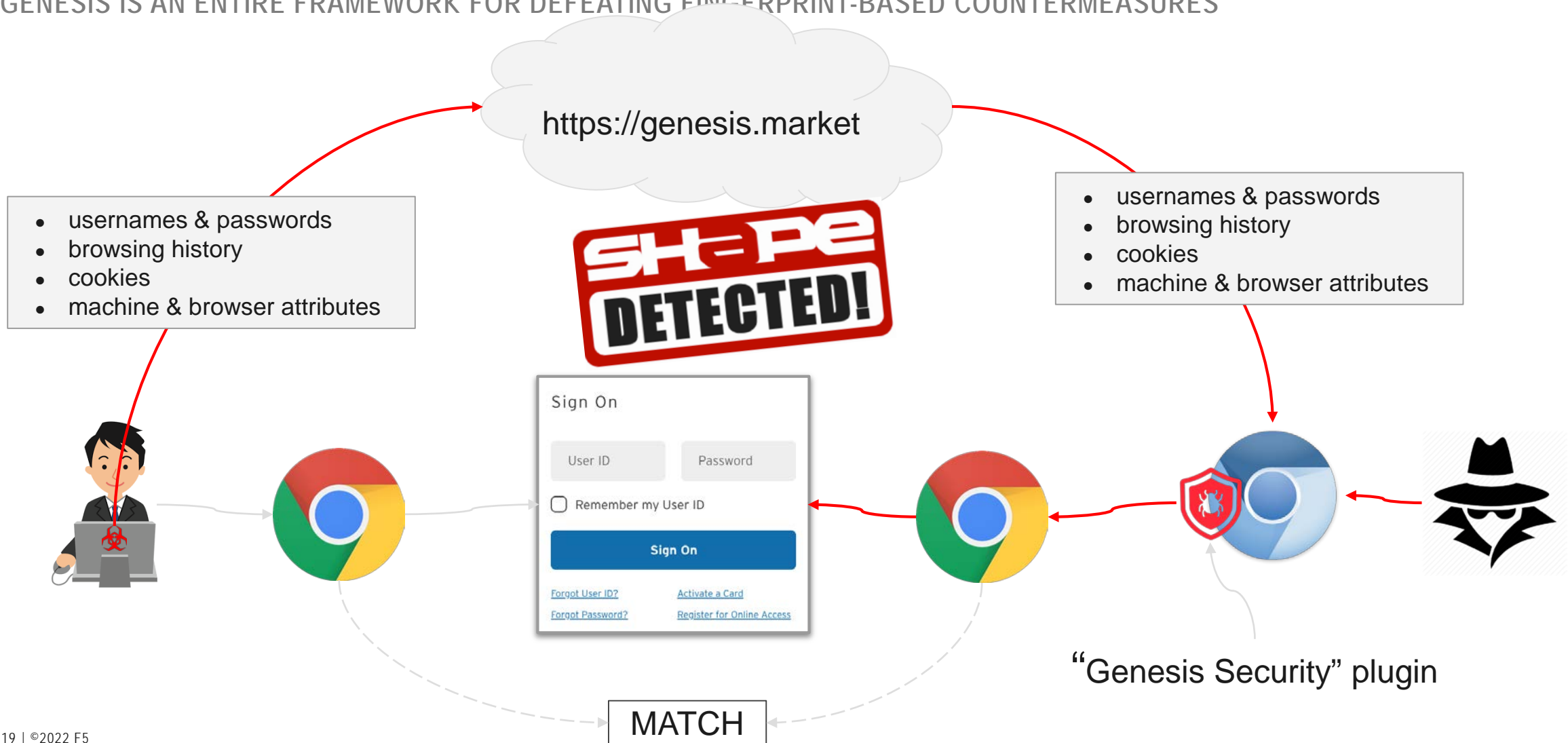
fromtheblocc

116 2

Genesis Crimeware

Genesis: the big picture

GENESIS IS AN ENTIRE FRAMEWORK FOR DEFEATING FINGERPRINT-BASED COUNTERMEASURES



Genesis digital fingerprint marketplace

The screenshot displays the Genesis digital fingerprint marketplace interface. The top navigation bar includes a 'genesis' logo and a menu icon. The left sidebar contains navigation options: Dashboard, Genesis Wiki (marked 'new'), News (10), Bots (127594), Generate FP, Orders, Purchases (1), Payments (4), Tickets (1), Genesis Security, Profile (4.7.3), Invites, and Logout.

The main content area is titled 'Bots' and features an 'Extended Search' button. Below the title, there are filter boxes for 'BOT NAME', 'RESOURCES KNOWN / OTHER', 'COUNTRY / HOST', and 'PRICE'. The main table lists bots for sale, with the first row highlighted by a red box. Each bot entry includes a unique ID, a 'NO INFO' status, a list of known resources, a price, and a 'Sale' badge.

BOT NAME	RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE
User-PC_4f8c81e4141433310c57	TDBank, iCloud, Dropbox, CanadianTireBank, UPS, BigCommerce, Kijiji, Skype, Google, Live	CA 207.210... Windows 7 SP1	163.00 81.50 Sale
4CEF4568-E5448574-3DA29599-D2ACE2A9-38CAF0F7	Wordpress, FedEx, Steam, Office365, Craigslist, Mypoints, Wellsfargo, PayPal, EANetwork, ATT	US 98.247... Windows 10 Home	50.00
A736D92B-9414907A-8BED9EBF-DA10D70F-BF36E648	Live, Yahoo, LinkedIn, 1and1WebMail, Twitter, Bittrex, OverstockStore, DigitalOcean, Messenger, Reddit	US 174.254... Windows 10 Enterprise	46.00

Genesis digital fingerprint marketplace



Dashboard Home / Bots

Genesis Wiki **new**

News 10 Bots

"Login": Available After Purchase
"Password": Available After Purchase

"Login": Available After Purchase
"Password": EMPTY

"Login": EMPTY
"Password": Available After Purchase

NO INFO

Twitter: 482 AppleStore: 1 = 484

Payments 4

Canada 163.00 81.50 207.210...

Know resources: 130

Google	15	Live	11	Amazon	8	PayPal	8	Facebook	7	DigitalOcean	7
Coinbase	7	Kraken	4	SonyEnter...	4	Twitter	3	Pof	3	Bitfinex	3
GoDaddy	3	TurboPrep...	3	Messenger	2	WIX	2	Netflix	2	PX Paxful	2
GitHub	2	Shopify	2	Intuit	2	Blockchain	2	Greendot	2	Steam	2
Bitcointalk	2	JuicyAds	2	Neteller	1	Cryptopay	1	GameStopS...	1	Yahoo	1
Reddit	1	Toluna	1	Bitstamp	1	MailGun	1	Overstock...	1	BigCommerce	1
Prizerebel	1	Bittrex	1	LinkedIn	1	1and1WebMail	1	Indeed	1	Wordpress	1
Instagram	1	Tradingview	1	Newegg	1	Comcast	1				

...other 1268

...known 130

...other 1268

Genesis digital fingerprint marketplace










The screenshot displays the Genesis digital fingerprint marketplace interface. A sidebar on the left contains navigation options: Dashboard, Genesis Wiki, News, Bots (127594), Generate FP (highlighted with a red box), Orders, Purchases (1), Payments (4), Tickets (1), Genesis Security (4.7.3), Profile, Invites, and Logout. The main content area features a green success banner: "Success generated FP is ready to use". Below this, the heading "Browsers for Genesis Security:" is followed by a list of browser configurations. The first configuration is for "chrome" (version 76.0.3809.132), which is checked. It includes details for cookies (419) and generated configs (1). A table lists the configuration details:

<input type="checkbox"/>	<input type="checkbox"/>	Cookies 419 (2019-09-14 20:11:43)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Generated Configs 1 :
	<i>Version</i>	Chrome 76 (Chrome 76.0.3809.132)
	<i>ConfigUpdate</i>	2019-09-21 17:21:39
	<i>UserAgent</i>	Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
	<i>Type</i>	generated (free)

At the bottom of the configuration list, there are two buttons: "Download in Genesis Security" (green) and "Open Bot page" (blue). The browser's address bar at the bottom shows "app.follow.unfollow", "com.acorns.android", and "...other 1268".

Genesis developers' loyalty is clear

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

	Azerbaijan
	Belarus
	Kazakhstan
	Kyrgyzstan
	Armenia
	Moldova
	Russia
	Tajikistan
	Uzbekistan

Dark Web Stats

Stats: Accounts for sale

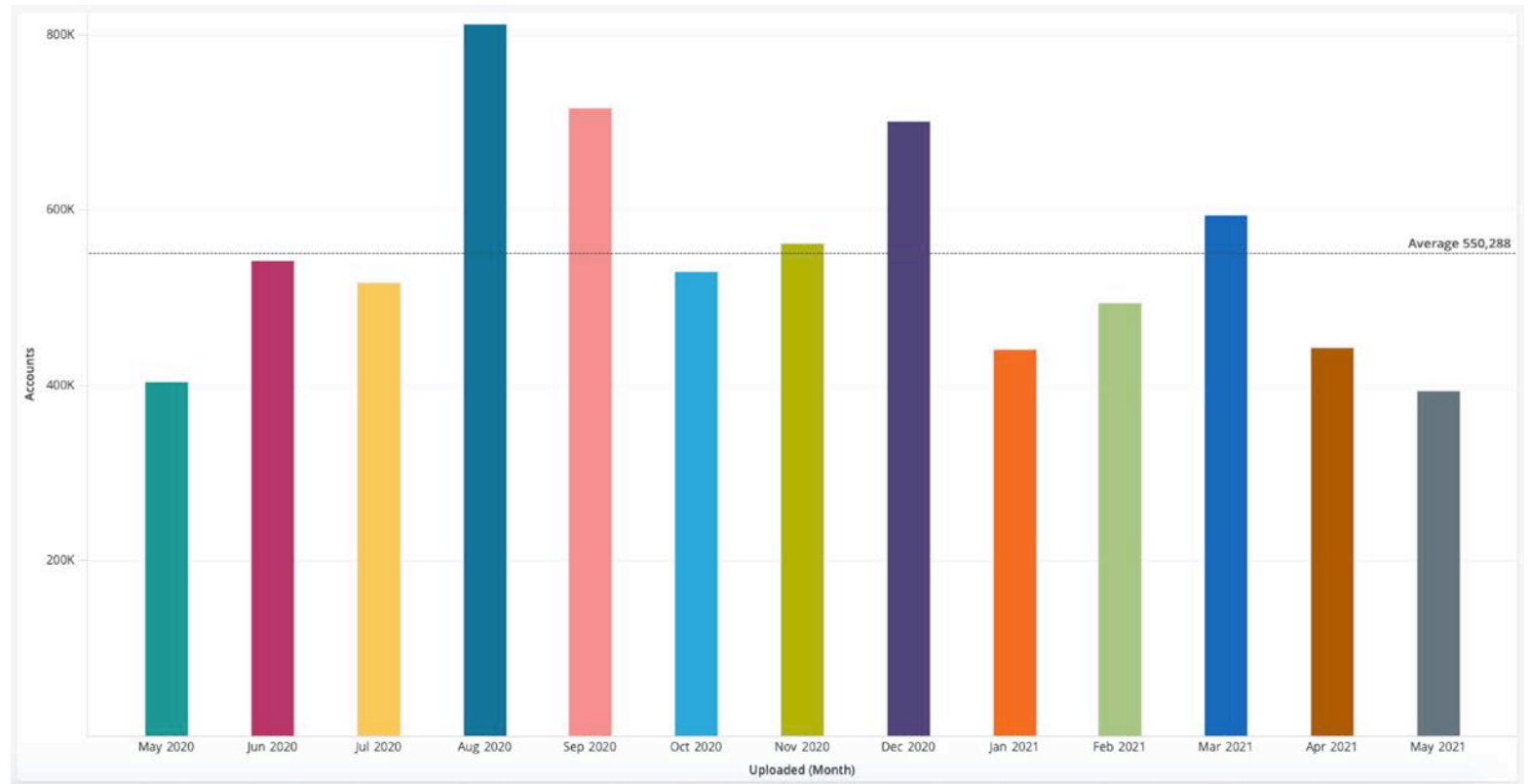
TAKEN FROM ONE DARK WEB SITE

Accounts For Sale
May 2020 – May 2021

720
Unique
Businesses

7.2M+
Accounts

\$20M+ in
Account
Costs



Stats: Top 40 Businesses with Accounts for Sale

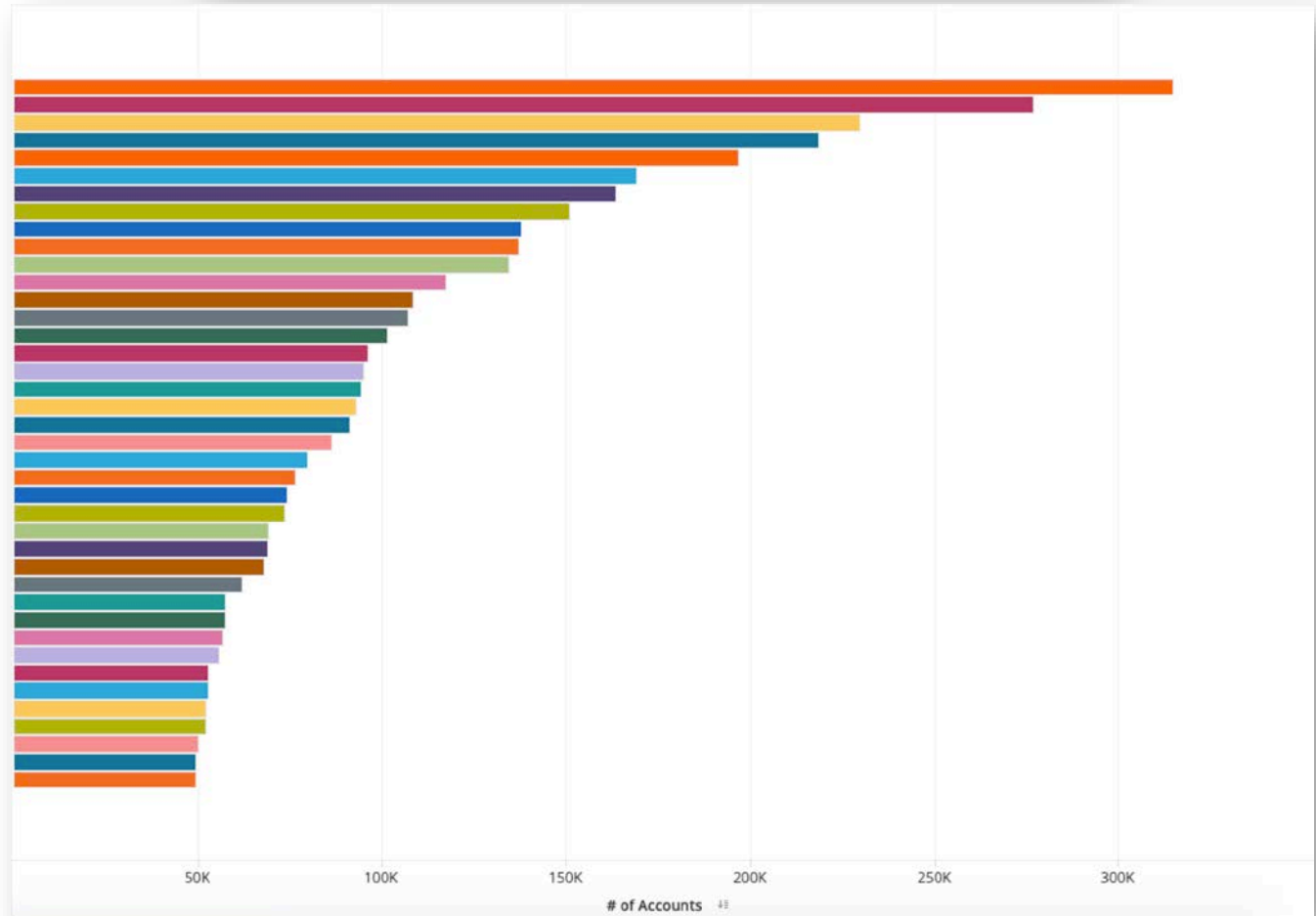
TAKEN FROM ONE DARK WEB SITE FOCUSED

Top 40 Businesses By Accounts
May 2020 – Mar 2021

#1 Spot
Over 300K+

Top 2-4
Over 200K+

Next 11
Over 100K+



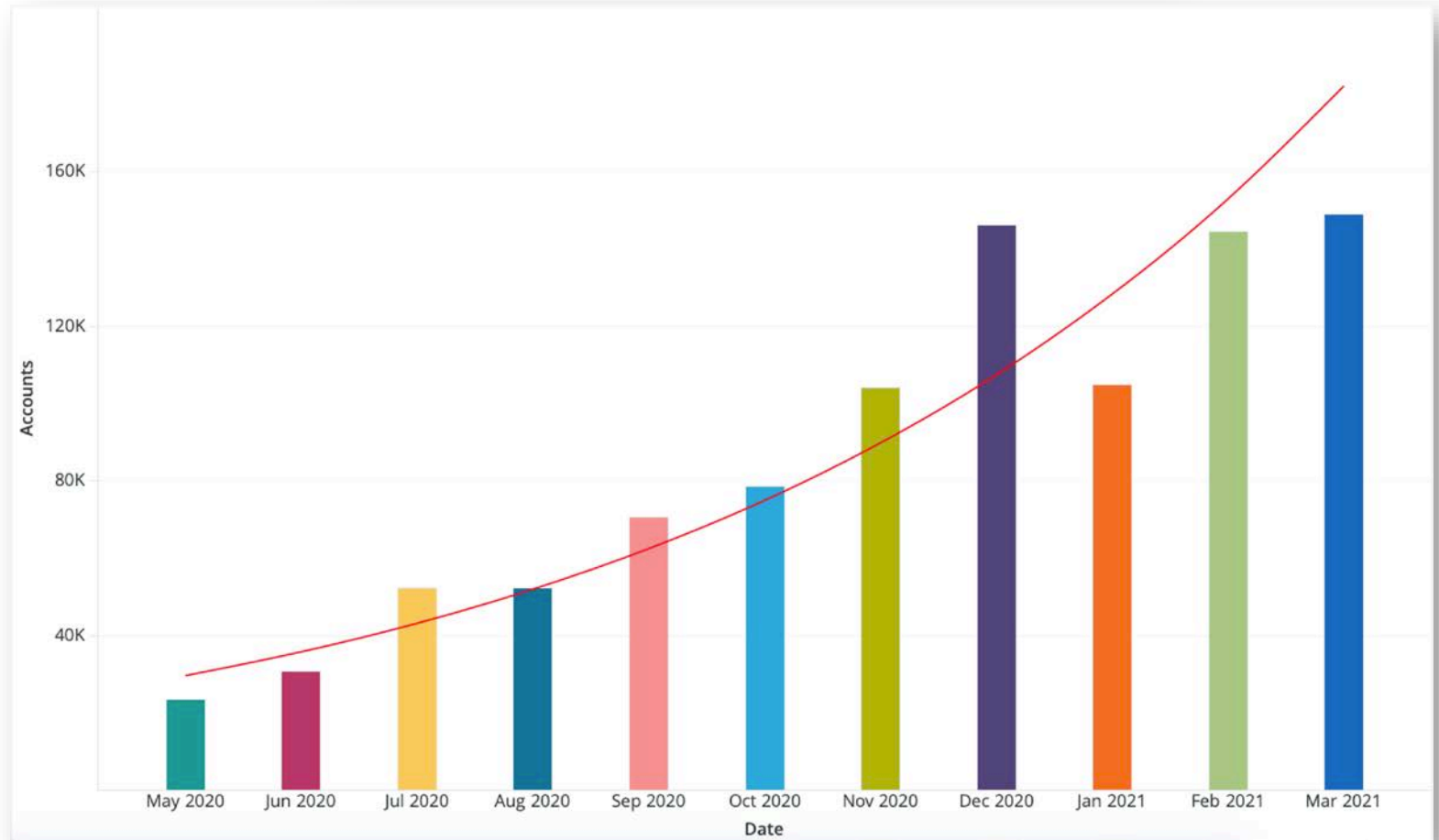
Stats: Mailbox ATO

DATA FROM ONE DARK WEB SITE

Mail ATO Accounts For Sale
May 2020 – Mar 2021

149K+
Accounts in
Feb

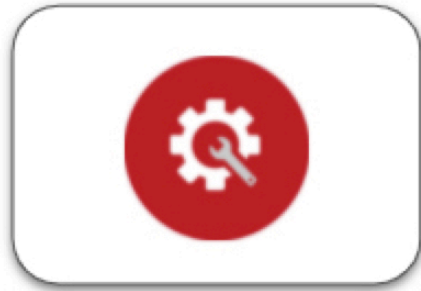
600%
Increase from
May -> Mar



Account Take Over (ATO) and Attack Tools Discussion

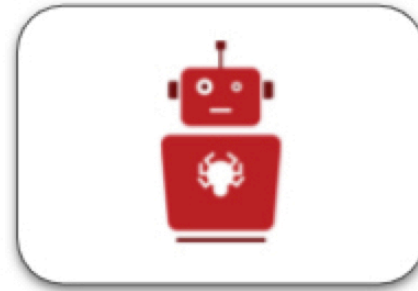
Credential Stuffing

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

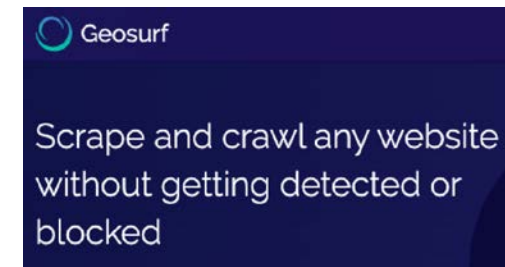
Combo List

- 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



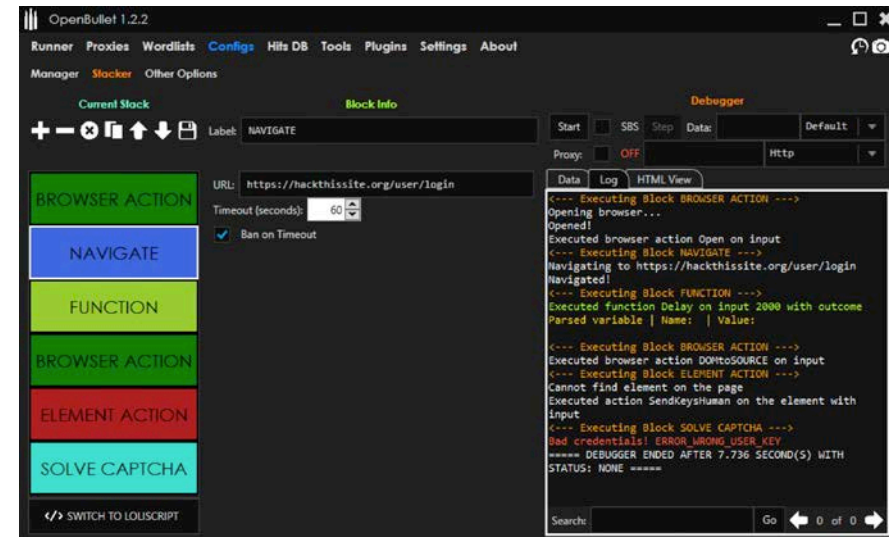
CURL / Bash Scripts

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

```
1 curl 'https://www.hackthissite.org/user/login' \  
2 -H 'authority: www.hackthissite.org' \  
3 -H 'pragma: no-cache' \  
4 -H 'cache-control: no-cache' \  
5 -H 'sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92" \  
6 -H 'sec-ch-ua-mobile: ?0' \  
7 -H 'upgrade-insecure-requests: 1' \  
8 -H 'origin: https://www.hackthissite.org' \  
9 -H 'content-type: application/x-www-form-urlencoded' \  
10 -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' \  
11 -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' \  
12 -H 'sec-fetch-site: same-origin' \  
13 -H 'sec-fetch-mode: navigate' \  
14 -H 'sec-fetch-user: ?1' \  
15 -H 'sec-fetch-dest: document' \  
16 -H 'referrer: https://www.hackthissite.org/user/login' \  
17 -H 'accept-language: en-US,en;q=0.9' \  
18 -H 'cookie: HackThisSite=lpqn46vm7ahhq83av1fkfr89i3' \  
19 --data-raw 'username=test&password=test' \  
20 --compressed
```

Attack toolkit – Openbullet

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



Openbullet

REMOTE BROWSER CONTROL WITH A GUI

Integrated Proxy Checker

Openbullet Demo

OpenBullet 1.2.2

Runner Proxies Wordlists Configs Hits DB Tools Plugins Settings About

Progress: [Progress bar] Bots: 1 [Slider]

Test On: + Success Key: +

Type	Host	Port	Username	Password	Country	Working	Ping	Chain	Last
Socks5	8.210.251.244	6666				YES	3908	False	7/5/2
Socks5	147.135.116.172	21610				YES	3936	False	7/4/2
Socks5	54.250.42.52	1080				YES	3881	False	7/4/2
Http	35.180.226.75	80				YES	4442	False	7/5/2
Socks5	97.74.230.87	47150				YES	2826	False	7/5/2
Socks5	52.47.81.82	1080				YES	4014	False	7/4/2
Socks5	147.135.112.67	3081				YES	3125	False	7/5/2
Http	128.199.150.84	8080				YES	4548	False	7/5/2
Socks5	195.144.21.185	1080				YES	5280	False	7/5/2
Http	185.38.111.1	8080				YES	3089	False	7/5/2
Http	114.121.248.251	8080				YES	4115	False	7/5/2
Socks5	210.77.87.71	10808				YES	7948	False	7/5/2
Http	140.227.65.3	6000				YES	4604	False	7/5/2
Http	145.239.6.118	3128				YES	4732	False	7/5/2
Http	78.157.40.35	998				YES	5128	False	7/5/2
Http	95.217.34.209	3128				YES	3763	False	7/5/2
Socks5	185.64.105.82	9050				YES	7558	False	7/5/2
Socks5	210.77.87.71	10808				YES	9271	False	7/4/2
Http	37.9.205.118	3128				YES	6647	False	7/5/2
Http	51.103.24.77	3128				YES	3244	False	7/5/2
Socks5	195.144.21.185	1080				YES	5865	False	7/4/2
Http	40.91.94.165	3128				YES	2012	False	7/5/2

CHECK

Import Export Delete Delete All More Actions

STATISTICS

Total: 26
Tested: 26
Working: 26
Not Working: 0
HTTP: 13
SOCKS4: 0
SOCKS4a: 0
SOCKS5: 13
Chain: 0

OPTIONS

Only Untested

Timeout (sec):

Runner Proxies Wordlists Configs Hits DB Tools Plugins Settings About

Manager Stacker Other Options

Current Stack

Label: BROWSER ACTION

Start SBS Step Data: [Dropdown] Default

Proxy: OFF HTTP

Data Log HTML View

Actions: Open

Input: [Text area]

```
<--- Executing block BROWSER ACTION --->
Opening browser...
Opened!
Executed browser action Open on input
<--- Executing block NAVIGATE --->
Navigating to https://www.google.com
Navigated!
<--- Executing block FUNCTION --->
Executed function Delay on input 2000 with outcome
Parsed variable | Name: | Value:
<--- Executing block ELEMENT ACTION --->
Executed action SendKeyshuman on the element with input Hello Google from Shape
Security, I'm a Robot!
<--- Executing block ELEMENT ACTION --->
Executed action Submit on the element with input
***** DEBUGGER ENDED AFTER 19.943 SECOND(S) WITH STATUS: NONE *****
```

SWITCH TO LOUSCRIPT

Opens the browser assigned to the current bot. This will be disregarded if the browser is already opened.

Search: [Text input] Go 0 of 0 Records

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**



```
root@kali:~# cd /root/.evilginx2 && ./evilginx -p ./phishlets/
```



Evilginx
no nginx - pure evil
by Kuba Gretzky (@mgretzky) version 2.0.0

```
08:23:56 [inf] loaded phishlet 'google' from 'google.yaml'  
08:23:56 [inf] setting up certificates for phishlet 'google'...  
08:23:56 [inf] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-almost-done.evilginx.com content.it-is-almost-done.evilginx.com]  
08:23:59 [inf] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36  
08:23:59 [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier  
sessions
```

id	phishlet	username	password	tokens	remote ip	time
19	google			none	192.168.1.100	2018-05-28 08:23

```
08:24:22 [inf] [0] Username: [REDACTED]  
08:24:29 [inf] [0] Password: [REDACTED]  
08:24:41 [inf] [0] all authorization tokens intercepted!  
08:24:41 [inf] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com  
sessions
```

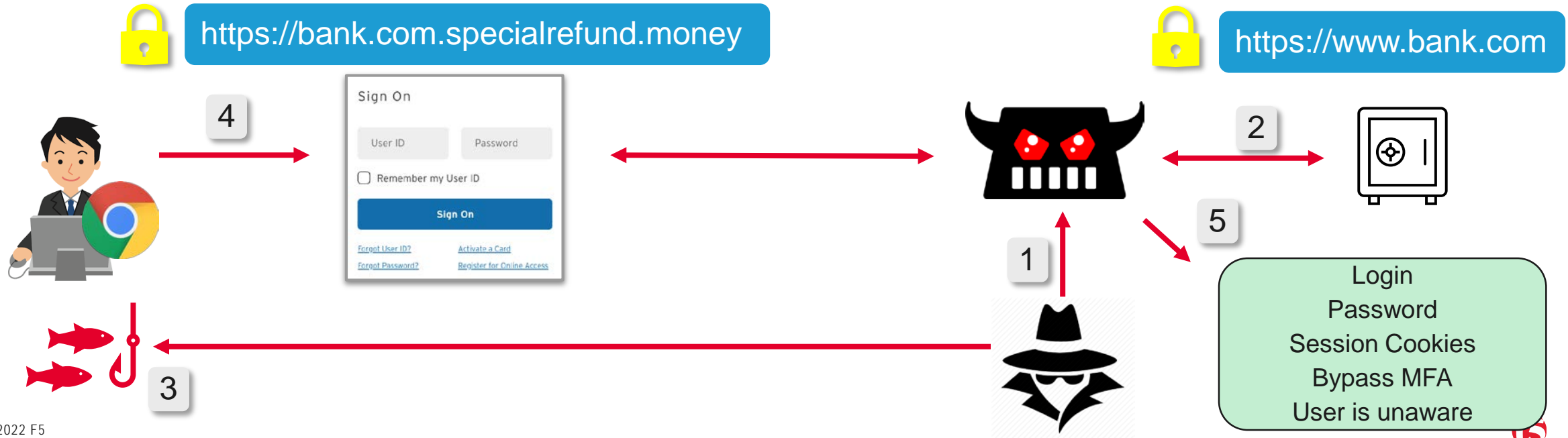
id	phishlet	username	password	tokens	remote ip	time
	google	[REDACTED]	[REDACTED]	captured	192.168.1.100	2018-05-28 08:24

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



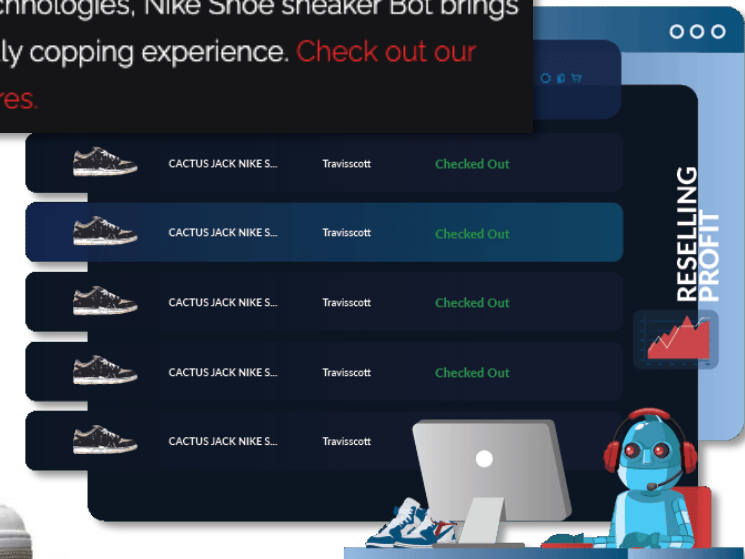
Nike Shoe Bot

(50 customer reviews)

\$499.00 / year

Snatch the latest limited sneakers like Jordans, NMDs, Yeezys, Off-Whites, Reflectives, Supreme and more off retailer's shelves and into your collection.

Using the latest automation technologies, Nike Shoe sneaker Bot brings you an efficient and user-friendly copping experience. [Check out our many new and improved features.](#)

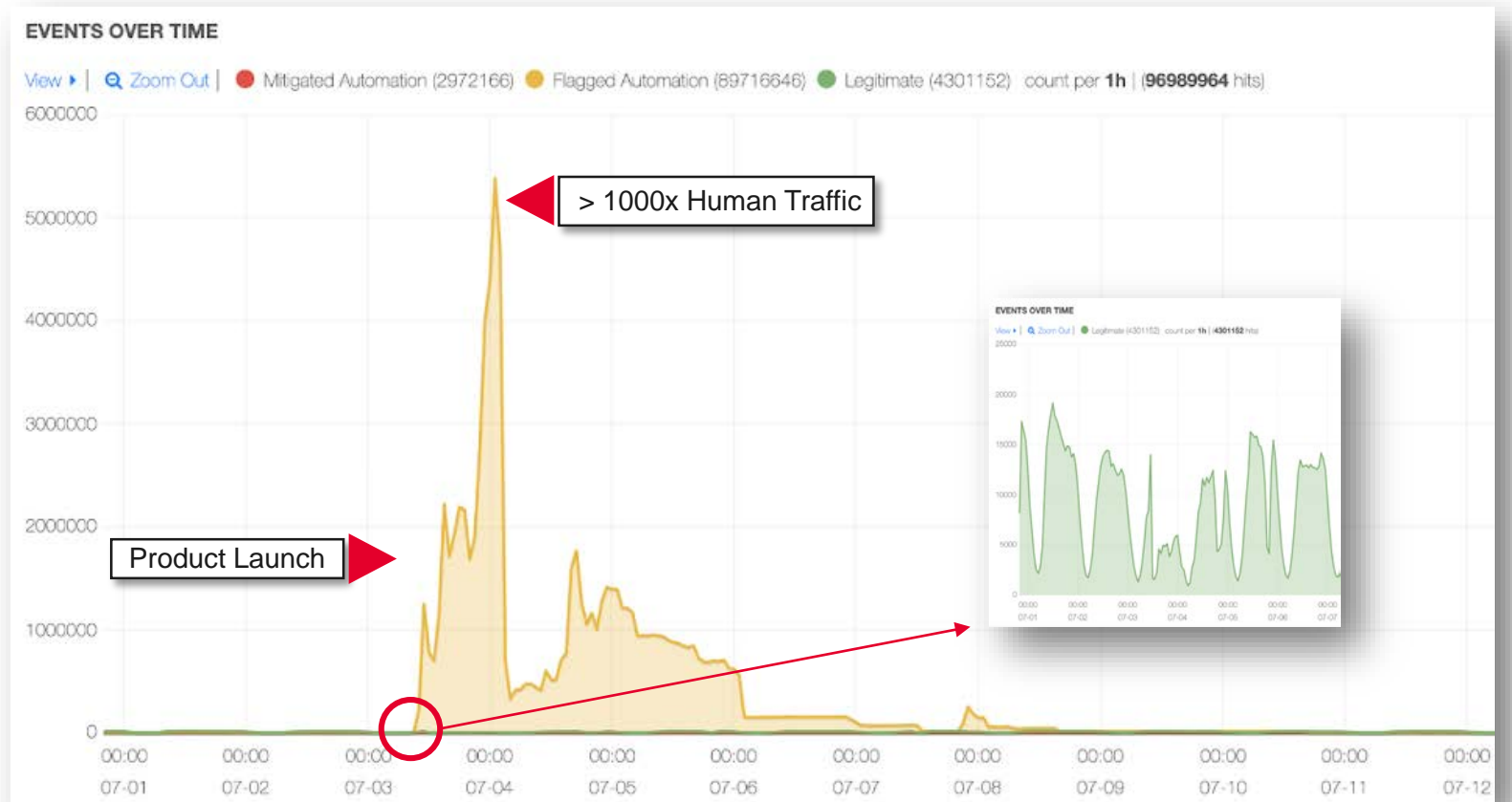


Example: Purchase Bots in Action

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

● Human ● Automation (flagged)



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

- Authentication Intelligence
- Account Protection (Anti Fraud)
- Client-Side Defense
- Advanced Bot Defense

WAAP

- Web Application Firewall
- API Security
- DDoS Mitigation
- Bot Defense

Integrated Services

- DNS
- Application Traffic Insight
- Load Balancing
- AppStack Managed Kubernetes
- Mesh Multi Cloud Infrastructure
- Customer Portal

F5 Distributed Cloud (SaaS)



The Power of F5 XC – Advanced App Security

FICTION

Identify and mitigate unwanted automation traffic



FRAUD

Differentiate good customers from bad customers



FRICION

Create a friction free user experience and increase revenue



Bots



*Human
Clickfarm*



*Fraudsters
and Criminals*



*Good
customers*

