Nethone

Evaluation of tools used to circumvent anti-fraud systems

March 25, 2020

MRC

Aleksander Kijek

Chief Product Officer
at Nethone

I am part of a passionate team of ~70 tech enthusiasts with top-class data science, engineering, and business skills

We gathered experience in world's top institutions

Google
EY
pwc
Palantir
L'ORÉAL
BCG
BIK Biuro Informacji Kredytowej
Deloitte.
Kontomatik Banking API
Goldman Sachs

Started to be internationally recognised

STATION F	**Participant** @ Thales Cybersecurity programme at STATION F **Paris, November '17 – April '18**
IATA	**Speaker** @ IATA Global Fraud Prevention **Madrid, September '18** **Miami, September '19**
PLUGANDPLAY	**Participant** @ Travel & Hospitality accelerator at Plug and Play **San Francisco, March - June '19**
MRC	**Member** of Merchant Risk Council **Since June '19**

And are trusted by many clients and organizations worldwide

eSky
Grover
Azul
ThalesAlenia Space
a Thales / Leonardo company
Polish Airlines LOT
automater
bitcan
FARFETCH

Agenda

What are the tools that fraudsters use for?

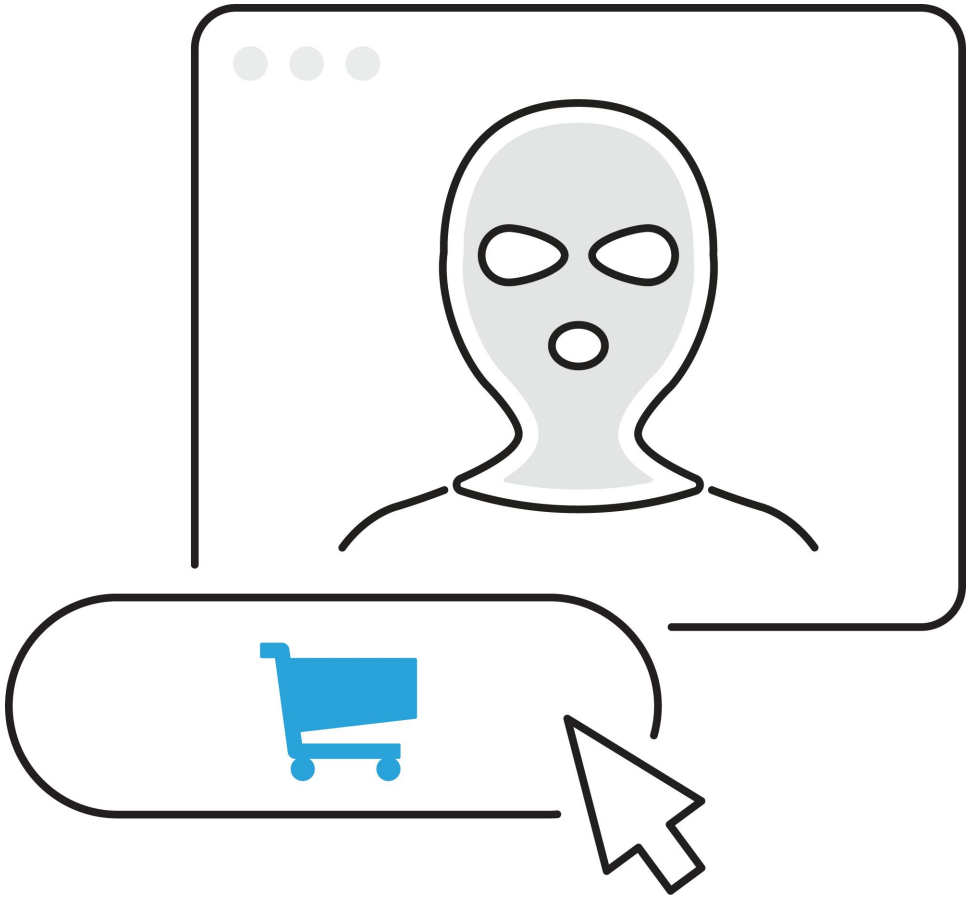
How do we know who sits in front of the computer?

Identifiers

Tools fraudsters use

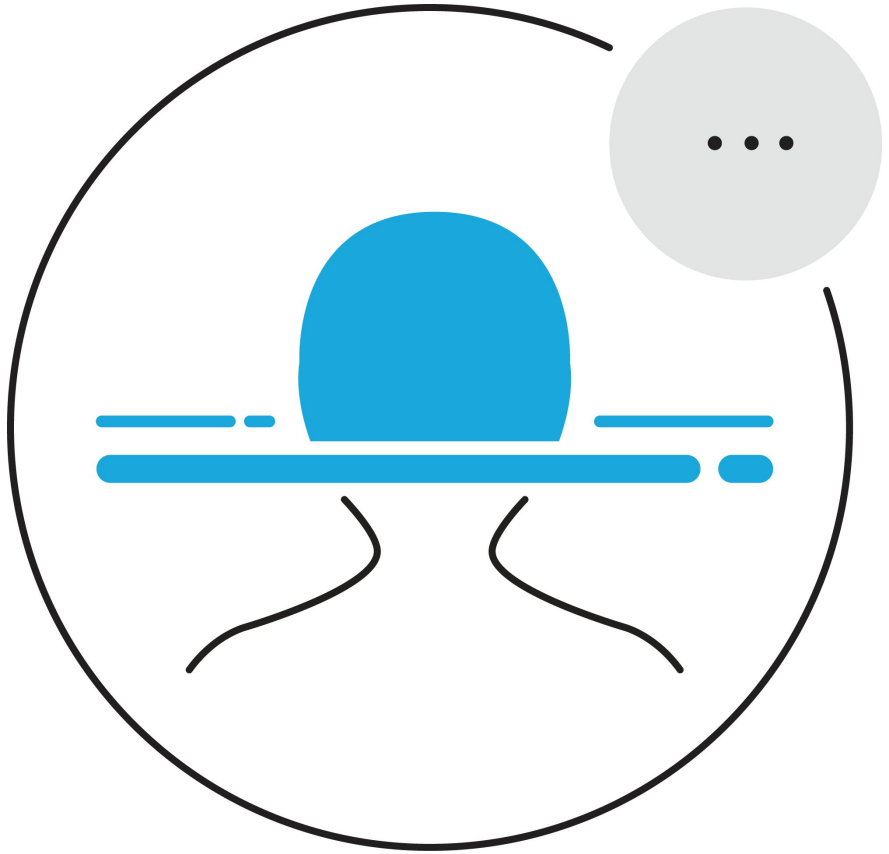
What are the fraud tools for?

- Anonymization – “I am a new client”
- Impersonation – “I am your trusted client”
- Phishing – “Let me be you” (conscious share of the victim)

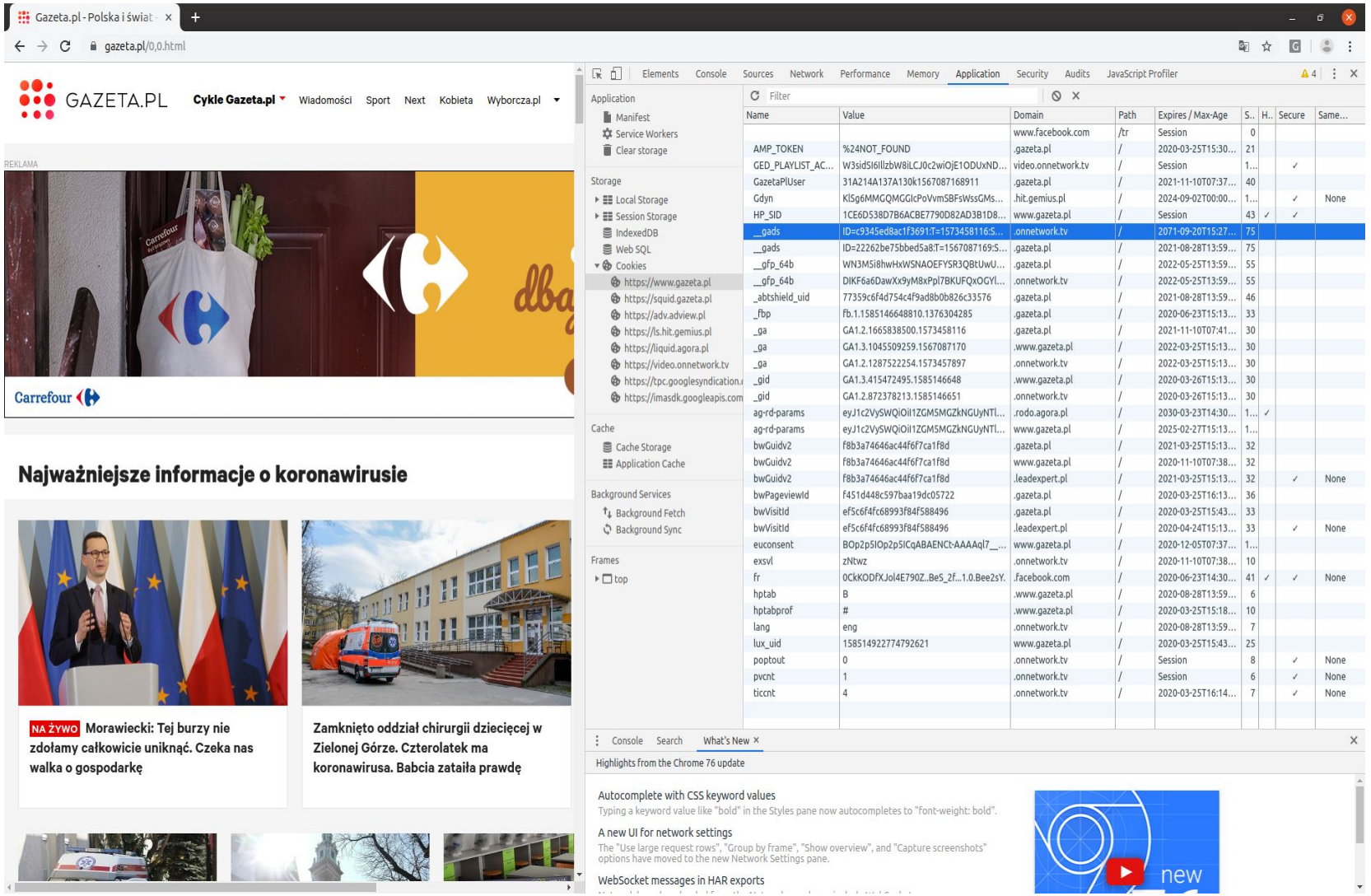


How do I know who it is?

- Cookie (stored on the device)
- Fingerprint (device configuration, behaviour)
- They tell me (login/password, card number)
- All of the above



Cookie – save it where you can



Fingerprint - so special but unique?

Hardware, software and browser intelligence

- GPU characteristics
- GPU detection
- Virtual machine detection
- Number of processor cores
- Mobile device detection
- Mobile emulation detection
- Battery
- Server OS detection
- DOM rendering engine anomalies
- HTML quirks
- Special cookies (based on HTML technologies, self regenerating)
- Popular fraudster's tools detection
- Spoofing detection
- Incognito mode detection
- Browser quirks
- Various fingerprints
- ...

Network characteristics

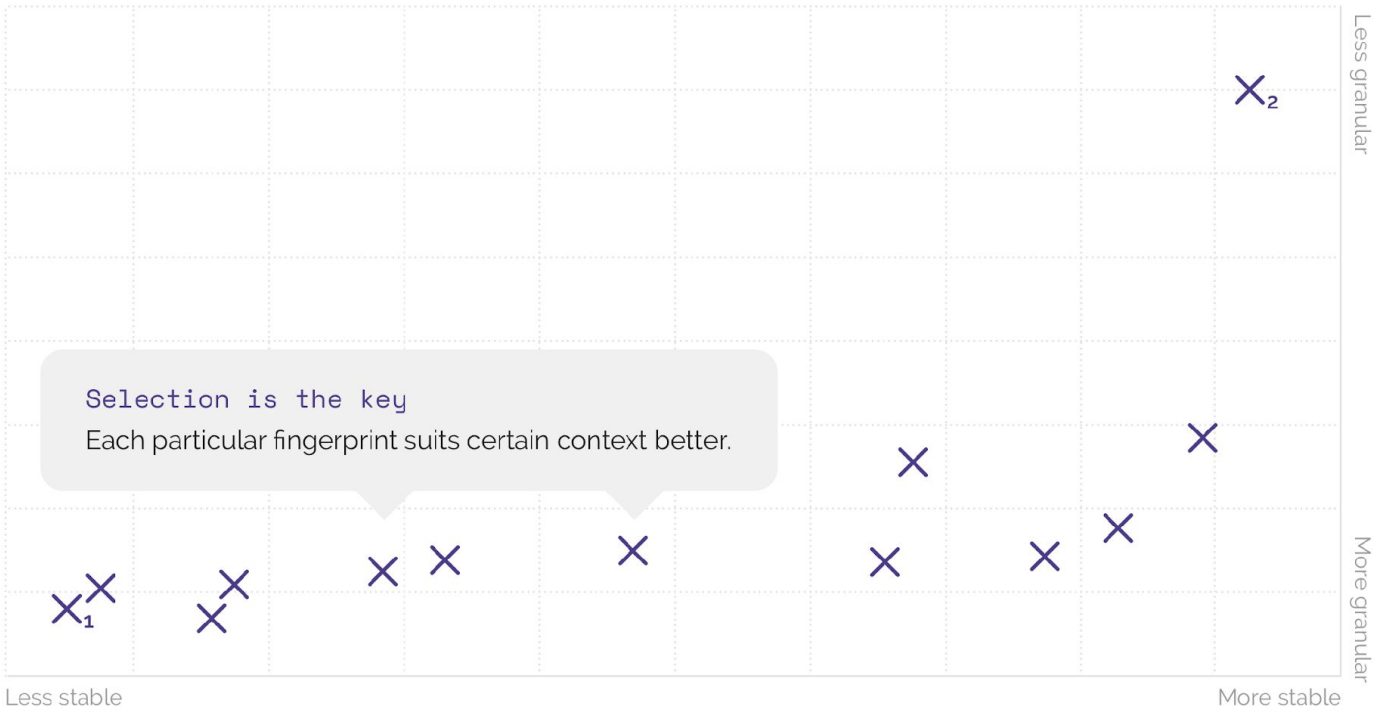
- IP geolocation
- TCP/IP stack analysis and anomalies detection
- Connection type detection (Wi-Fi, cellular) based on low level network analysis and/or browser features checks
- OS Fingerprinting
- VPN/Proxy/Tunnelling detection
- Tor detection
- Public IP leak /Local IP leak
- Server-based connection detection
- ....

Raw behavioural data

- Mouse/Touchpad movements
- Swipes/Touches or scrolls
- Keystroke dynamics
- Gyro readings
- Accelerometer
- Clipboard usage
- ...

Fingerprint – immortal but the same

Fingerprints' granularity vs stability

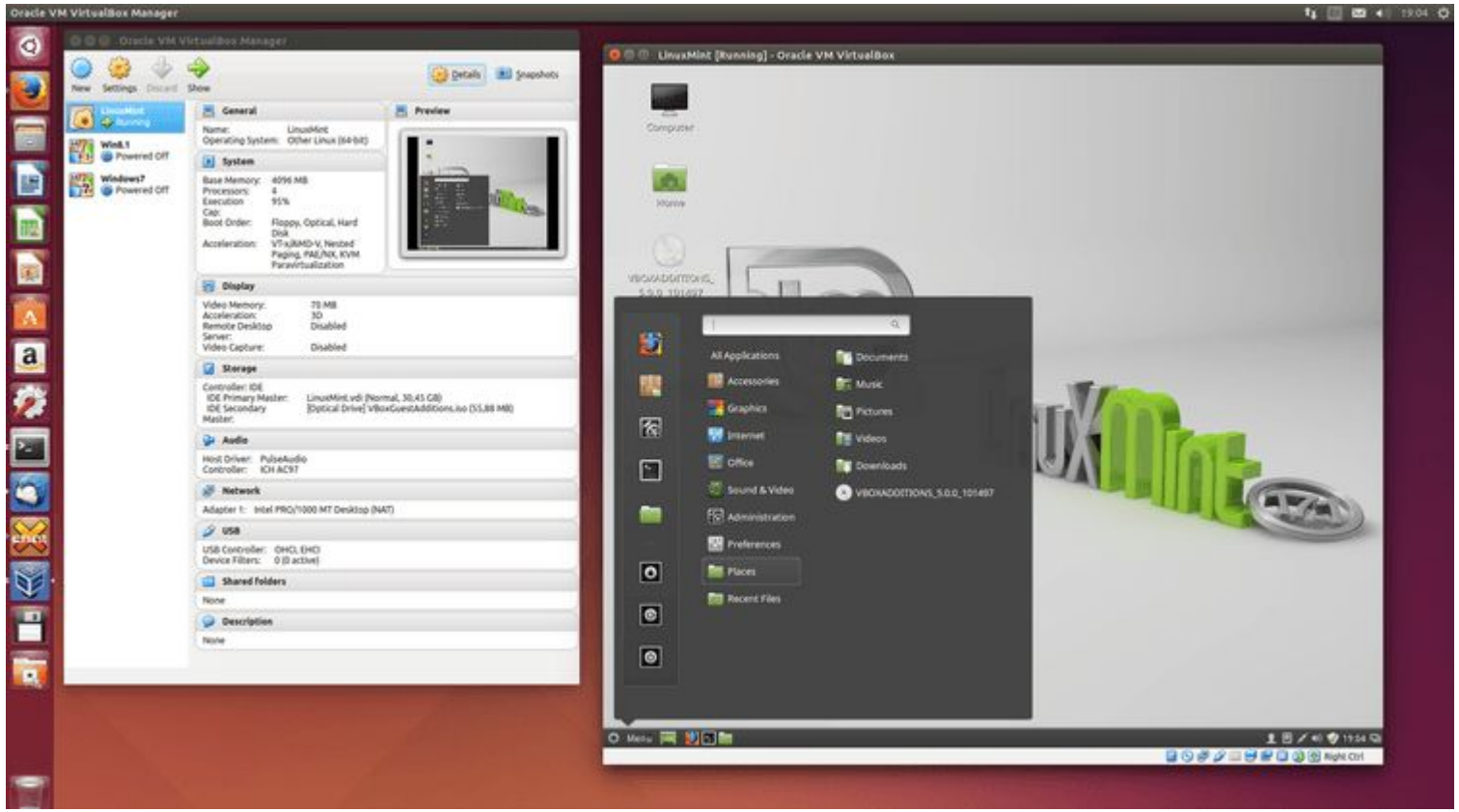


X_1 is a fingerprint of small stability, but high granularity. | X_2 is a fingerprint of big stability, but low granularity.

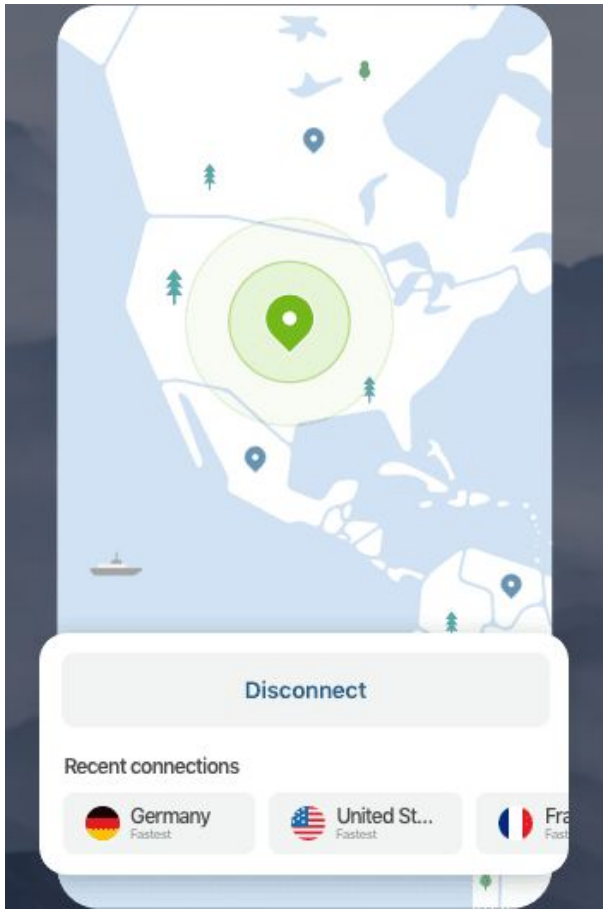
Tools the fraudsters use

- Virtual Machine, VPN, TORBrowser – free
- FraudFox, AntiDetect, LinkenSphere - paid
- Fake websites, Fake services, Muraena + Necrobrowser – self development and targeted

Virtual Machine, VPN, TORBrowser - not malicious by design

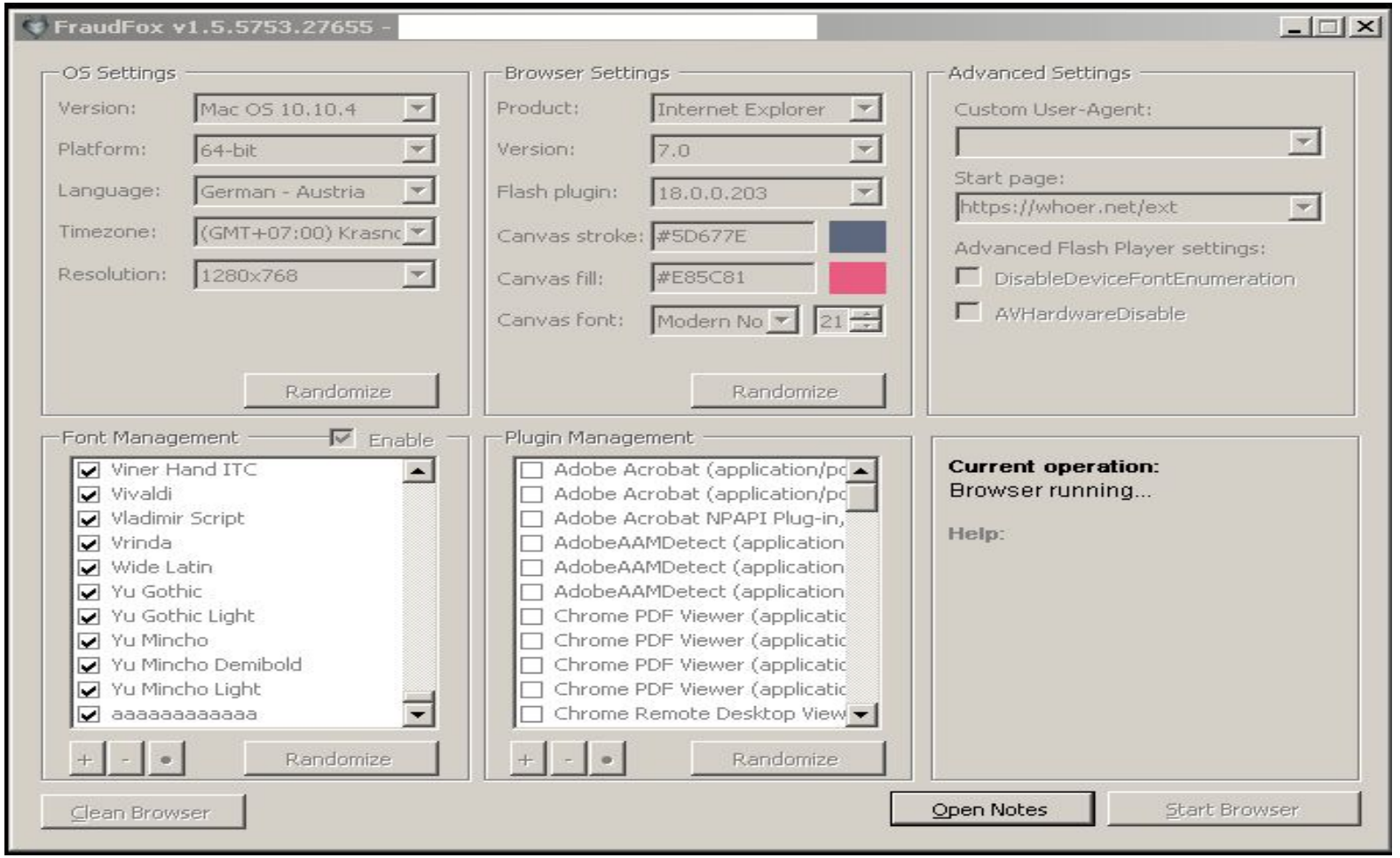


Source: www.virtualbox.org

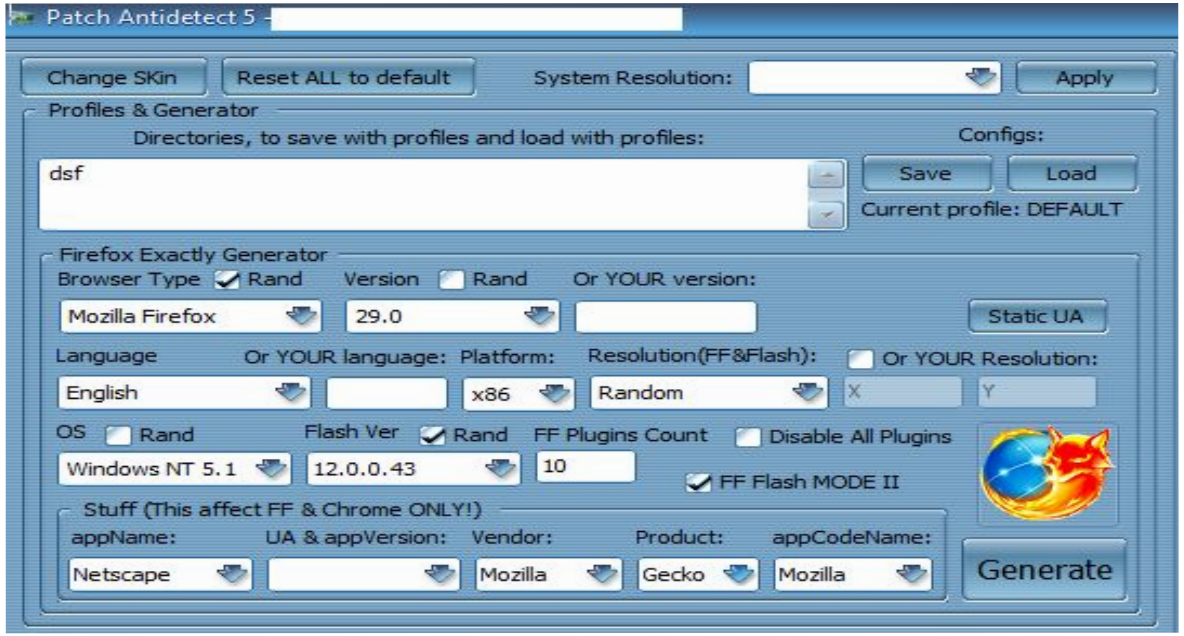


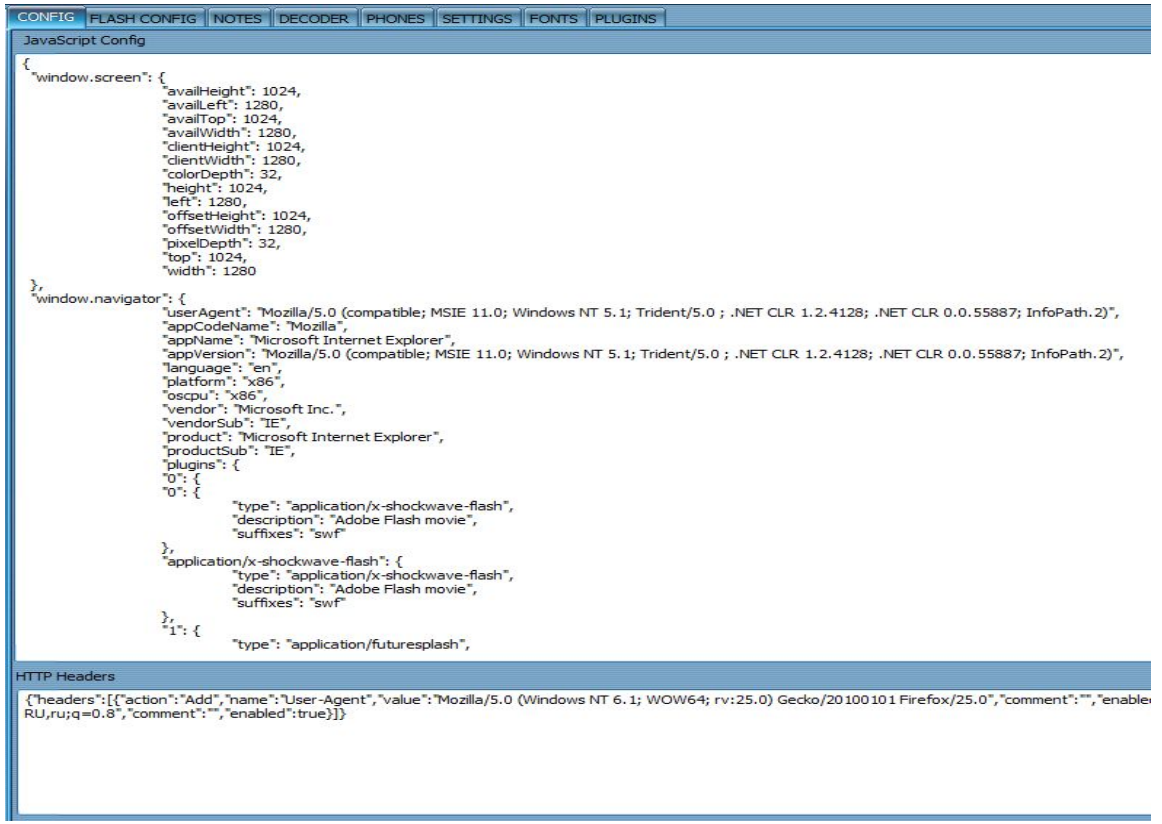
Source: nordvpn.com

Fraudfox


FraudFox v1.5.5753.27655 -
OS Settings
Version: Mac OS 10.10.4
Platform: 64-bit
Language: German - Austria
Timezone: (GMT+07:00) Krasnc
Resolution: 1280x768
Randomize
Browser Settings
Product: Internet Explorer
Version: 7.0
Flash plugin: 18.0.0.203
Canvas stroke: #5D677E
Canvas fill: #E85C81
Canvas font: Modern No 21
Randomize
Advanced Settings
Custom User-Agent:
Start page: https://whoer.net/ext
Advanced Flash Player settings:
DisableDeviceFontEnumeration
AVHardwareDisable
Font Management
Enable
Viner Hand ITC
Vivaldi
Vladimir Script
Vrinda
Wide Latin
Yu Gothic
Yu Gothic Light
Yu Mincho
Yu Mincho Demibold
Yu Mincho Light
aaaaaaaaaaaa
Randomize
Plugin Management
Adobe Acrobat (application/pd
Adobe Acrobat (application/pd
Adobe Acrobat NPAPI Plug-in,
AdobeAAMDetect (application
AdobeAAMDetect (application
AdobeAAMDetect (application
Chrome PDF Viewer (applicatic
Chrome PDF Viewer (applicatic
Chrome PDF Viewer (applicatic
Chrome PDF Viewer (applicatic
Chrome Remote Desktop View
Randomize
Current operation:
Browser running...
Help:
Clean Browser
Open Notes
Start Browser

Antidetect


Patch Antidetect 5
Change SKin
Reset ALL to default
System Resolution:
Apply
Profiles & Generator
Directories, to save with profiles and load with profiles:
Configs:
dsf
Save
Load
Current profile: DEFAULT
Firefox Exactly Generator
Browser Type
Rand
Version
Rand
Or YOUR version:
Mozilla Firefox
29.0
Static UA
Language
Or YOUR language:
Platform:
Resolution(FF&Flash):
Or YOUR Resolution:
English
x86
Random
X
Y
OS
Rand
Flash Ver
Rand
FF Plugins Count
Disable All Plugins
Windows NT 5.1
12.0.0.43
10
FF Flash MODE II
Stuff (This affect FF & Chrome ONLY!)
appName:
UA & appVersion:
Vendor:
Product:
appCodeName:
Netscape
Mozilla
Gecko
Mozilla
Generate


CONFIG
FLASH CONFIG
NOTES
DECODER
PHONES
SETTINGS
FONTS
PLUGINS
JavaScript Config
{
"window.screen": {
"availHeight": 1024,
"availLeft": 1280,
"availTop": 1024,
"availWidth": 1280,
"clientHeight": 1024,
"clientWidth": 1280,
"colorDepth": 32,
"height": 1024,
"left": 1280,
"offsetHeight": 1024,
"offsetWidth": 1280,
"pixelDepth": 32,
"top": 1024,
"width": 1280
},
"window.navigator": {
"userAgent": "Mozilla/5.0 (compatible; MSIE 11.0; Windows NT 5.1; Trident/5.0 ; .NET CLR 1.2.4128; .NET CLR 0.0.55887; InfoPath.2)",
"appCodeName": "Mozilla",
"appName": "Microsoft Internet Explorer",
"appVersion": "Mozilla/5.0 (compatible; MSIE 11.0; Windows NT 5.1; Trident/5.0 ; .NET CLR 1.2.4128; .NET CLR 0.0.55887; InfoPath.2)",
"language": "en",
"platform": "x86",
"oscpu": "x86",
"vendor": "Microsoft Inc.",
"vendorSub": "IE",
"product": "Microsoft Internet Explorer",
"productSub": "IE",
"plugins": {
"0": {
"0": {
"type": "application/x-shockwave-flash",
"description": "Adobe Flash movie",
"suffixes": "swf"
},
"application/x-shockwave-flash": {
"type": "application/x-shockwave-flash",
"description": "Adobe Flash movie",
"suffixes": "swf"
},
"1": {
"type": "application/futuresplash",
HTTP Headers
{"headers":[{"action":"Add","name":"User-Agent","value":"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0","comment":"","enable
RU,ru;q=0.8","comment":"","enabled":true}]}

Sphere – digital multi-identity tool

It is absolute security, anonymity and freedom.

Hundreds of new identities just in one click

The browser has systems for protection and fingerprint substitution (GPU, Audio, Canvas, Plugins, Fonts, ClientRects, Ubercookies) automatically changing them for each new identity. Nobody can recognize configuration of your real computer if you surf with Sphere – it protects you against any identification attempt.

AES-256 encryption

The browser uses the best protected type of data encryption to keep safe information saved to the computer in case of necessity. Besides, you can import identities with necessary data safely.

Portable format

Portable format of the software allows using it where it is necessary without installing it to the computer. You can easily run Sphere from a protected drive or from a private section of the computer – it is the most secure solution among the all-in-one browsers existing today.

OTR-mode

Sphere operates in Off-the-Record mode – during software operation all current files and data are saved in RAM till its closure. Thus, it is impossible to get access to information about visited sites and activities in them even using spying solutions (viruses) installed directly on the computer.

Anonymity in the Internet

The software allows you easily substitute your IP-address using, e.g., TOR. The users who do not trust an onion network can make use of multiflow SOCKS and SSH connections. You are everywhere and nowhere at the same time.

Absence of spying code

Sphere is designed using Chromium core, but it is totally devoid of all elements of Google spying code, which is impossible to completely delete or disable in any out-of-box browser solutions. Be sure of your own safety and anonymity.

https://sphere.tenebris.cc/

Muraena + Necrobrowser – 2FA based on a cookie no more

https://github.com/muraenateam/muraena

YOUR LOGO HERE

help us with a logo

Release license BSD3 go report A

Muraena is an almost-transparent reverse proxy aimed at automating phishing and post-phishing activities.

The tool re-implements the 15-years old idea of using a custom reverse proxy to dynamically interact with the origin to be targeted, rather than maintaining and serving static pages.

Written in Go, Muraena does not use slow-regexes to do replacement magic, and embeds a crawler (Colly) that helps determining in advance which resource should be proxied.

Muraena does the bare minimum to grep/replace origins in request/responses: this means that for complex origins extra manual analysis might be required to tune the auto-generated JSON configuration file. Hence, do not expect the reverse proxy to work straight out of the box for complex origins.

The config folder has some examples of custom replacements needed on complex origins likes GSuite, Dropbox, GitHub and others.

Documentation

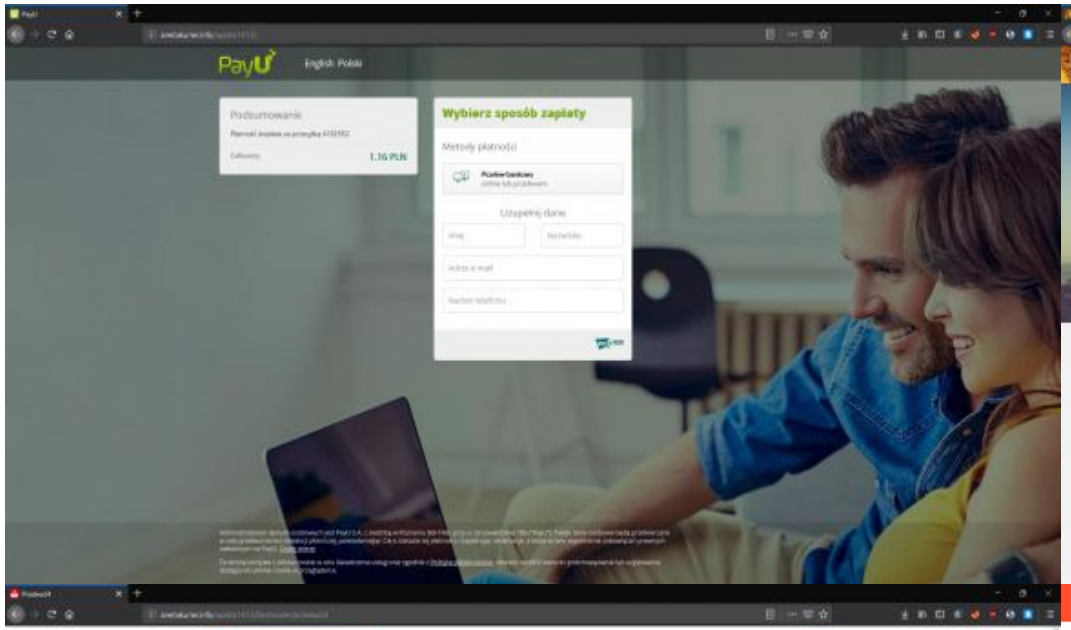
The project is documented in the Wiki here.

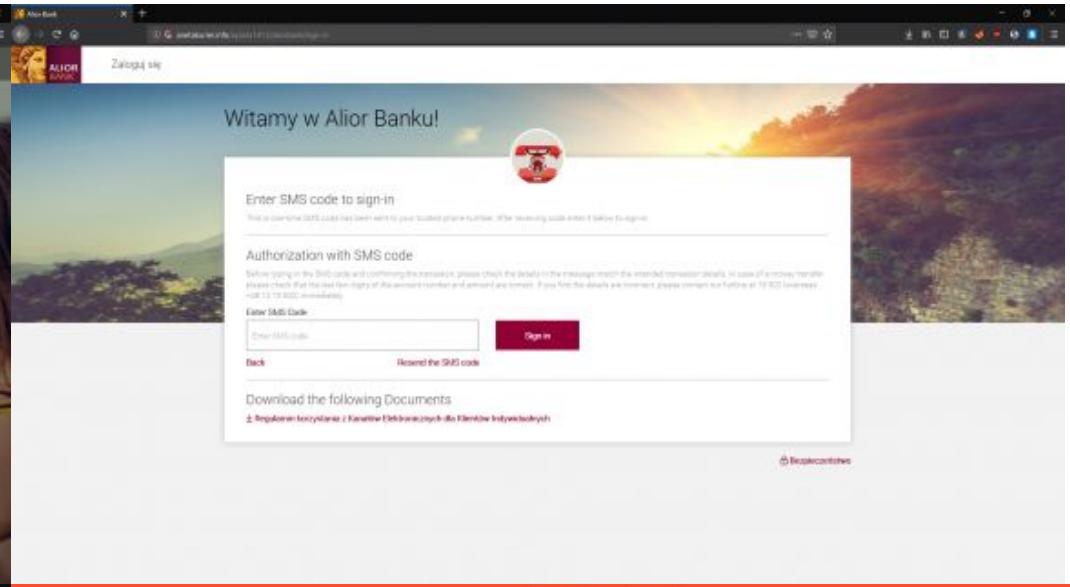
Contributing

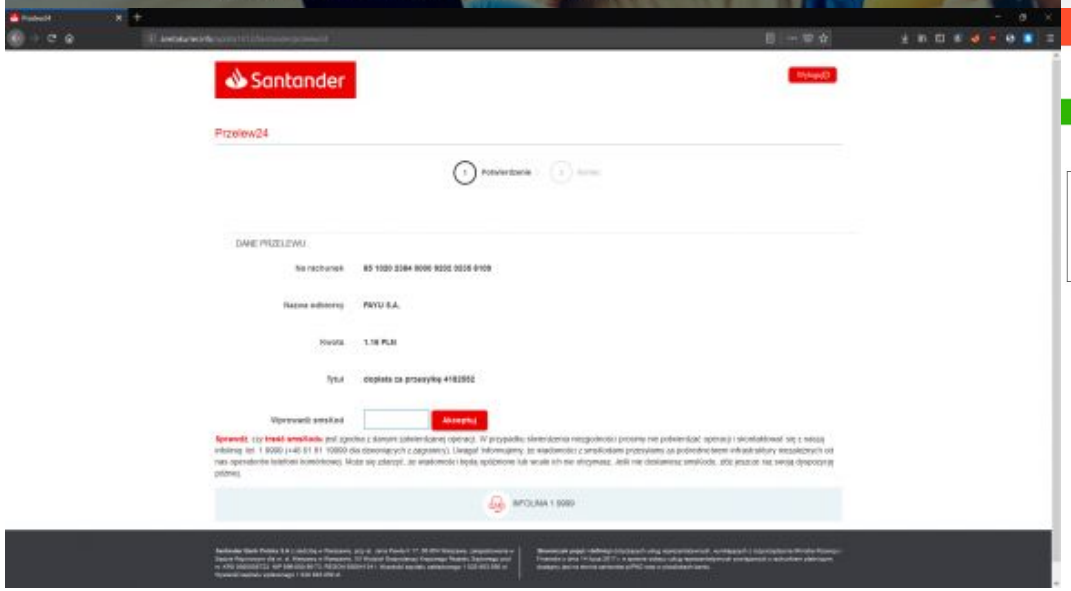
1. Fork it!
2. Create your feature branch: `git checkout -b my-new-feature`
3. Commit your changes: `git commit -am 'Add some feature'`
4. Push to the branch: `git push origin my-new-feature`
5. Submit a pull request 😍

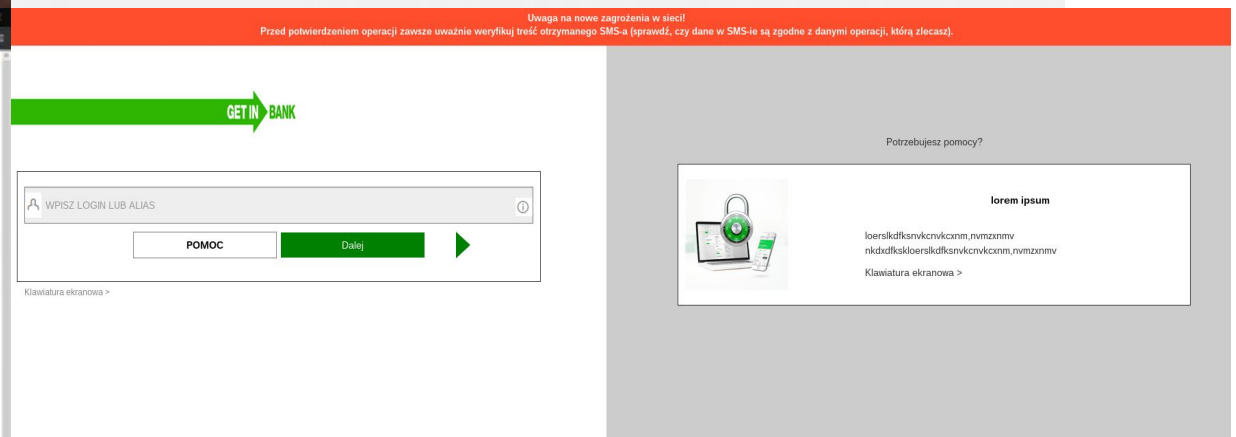
See the list of contributors who participated in this project.

Fake websites, fake services – phishing and creativity



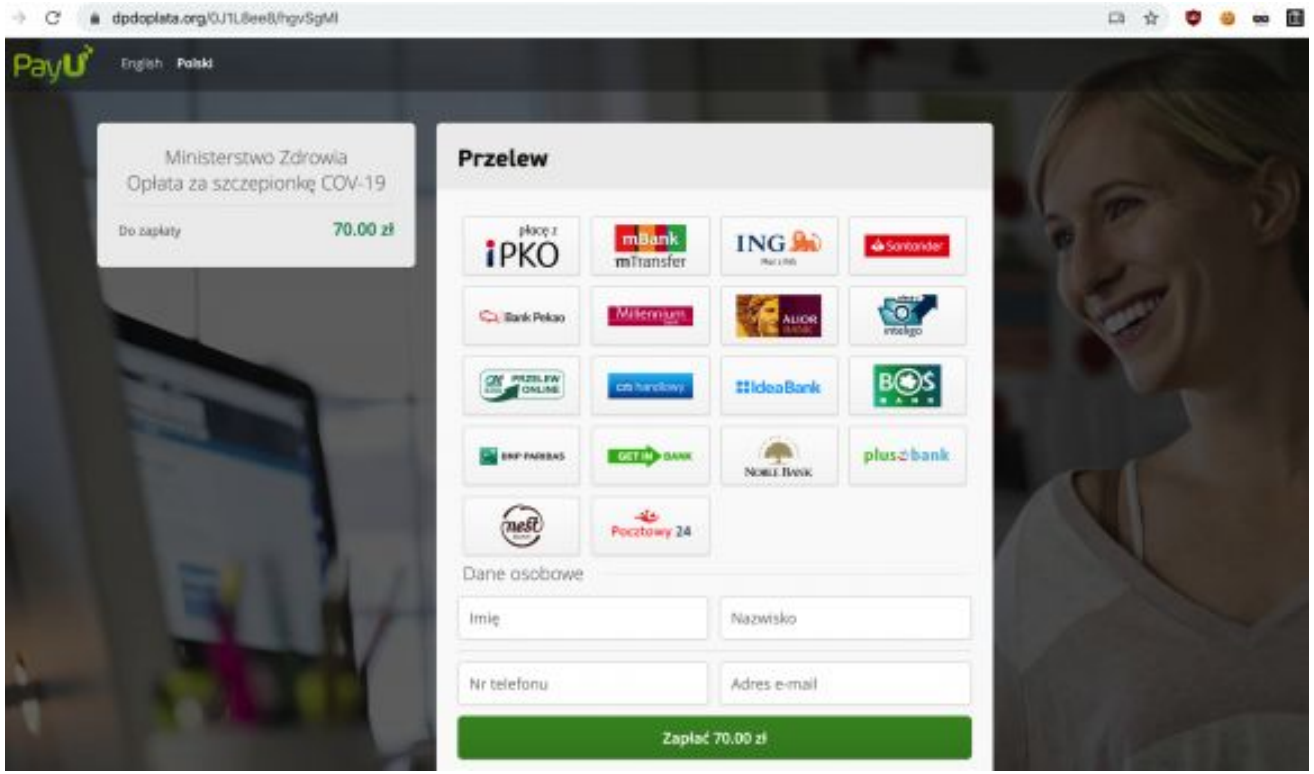






Source: zaufanatrzeciastrona.pl

Opportunities

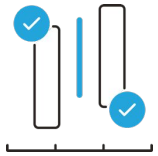


Source: zaufanatrzeciastrona.pl

Carding market's answer to the PSD2 - arms race never stops

It is expected that fraud orientated businesses that are able spend lots of money will be creating new tools to omit the 2FA

Therefore, anti-fraud solution providers must be both reactive and foreseeing.



Know Your Users

Fraud prevention

Exhaustive digital image

End User

Frictionless 3FA

- Enhanced **feeling of safety** at no additional cost
- Client satisfaction – **zero friction, 100% safety**

Merchant

Financial benefits

- Additional safety layer in the IT SEX technology stack
- Considerably reduced ATO risk
- Lower operational costs

Feel free to get in touch,
I am happy to discuss further!

+48 793 013 302

aleksander.kijek@nethone.com