Ochrana proti webovému fraudu

Září 2021

Filip Kolář, f.kolar@f5.com

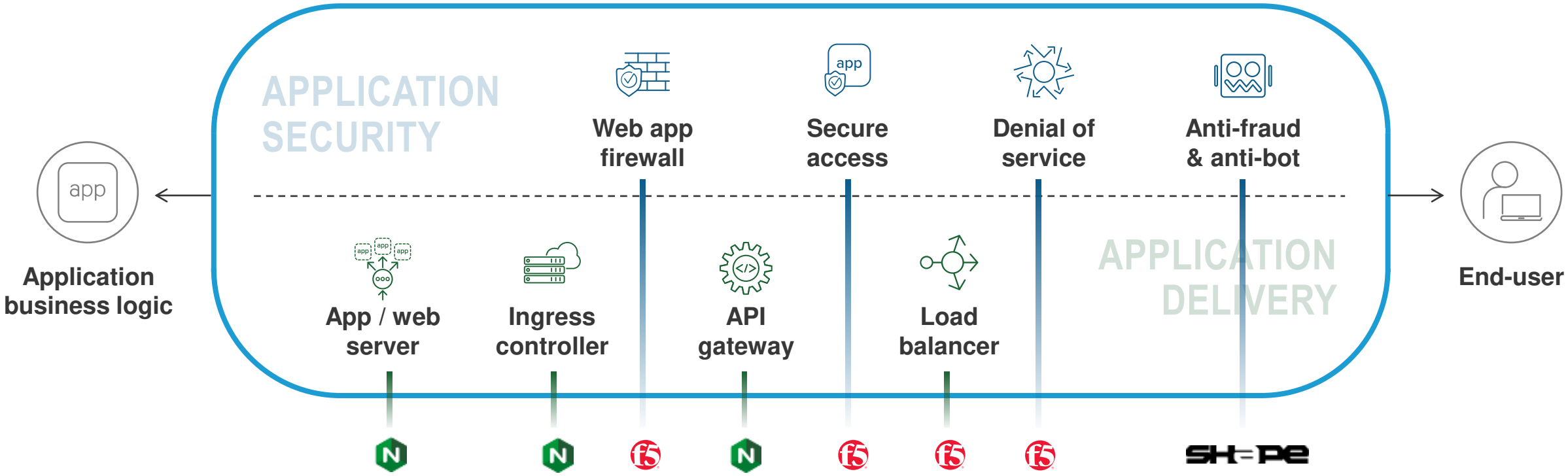
F5 Česká republika

ISSS

Zákazníci v ČR a na Slovensku – více než 200 instalací

- Finance – Banky, nebankovní instituce, platební brány
- Komerční sektor – Sázkové kanceláře, utility, …
- Operátoři – Telco, ISP, poskytovatelé „manageovaných“ služeb
- Státní správa a podniky - Ministerstva, kraje, velké státní podniky

The F5 portfolio nabízí na trhu to nejlepší z oblasti app delivery s benefitem snížení komplexity a nákladů



The F5 portfolio nabízí na trhu to nejlepší z oblasti app delivery s benefitem snížení komplexity a nákladů

BIG-IP

Simplify traditional app delivery for multi-cloud

BIG-IP

NGINX

Enable modern app delivery at scale

NGINX
Part of F5

SHAPE / SILVERLINE

Secure and app insight anywhere

F5 Security + SHAPE Part of F5

Volterra

EDGE 2.0

CLOUD SERVICES / VOLTERRA

Shape Security – ochrana proti webovým podvodům

Webové podvody: Převzetí účtu / identity

Útočníci využívají zákaznických profilů obětí + automatizační framework pro imitaci reálného provozu

Attackers are abusing **inherent functionality** to conduct automated & manual fraud

Credential Stuffing!
100,000 pokusů o Account Taker-Over může stát pouhých $200

$0

2.3 billion credentials

$0-50

For tool configuration

$0-139

For 100,000 solved CAPTCHAs

$0-10

For 1,000 global IPs

< $0.002

per ATO attempt.

Credential Stuffing
Krok 1: Získání uživatelských jmen a hesel

PHISHING

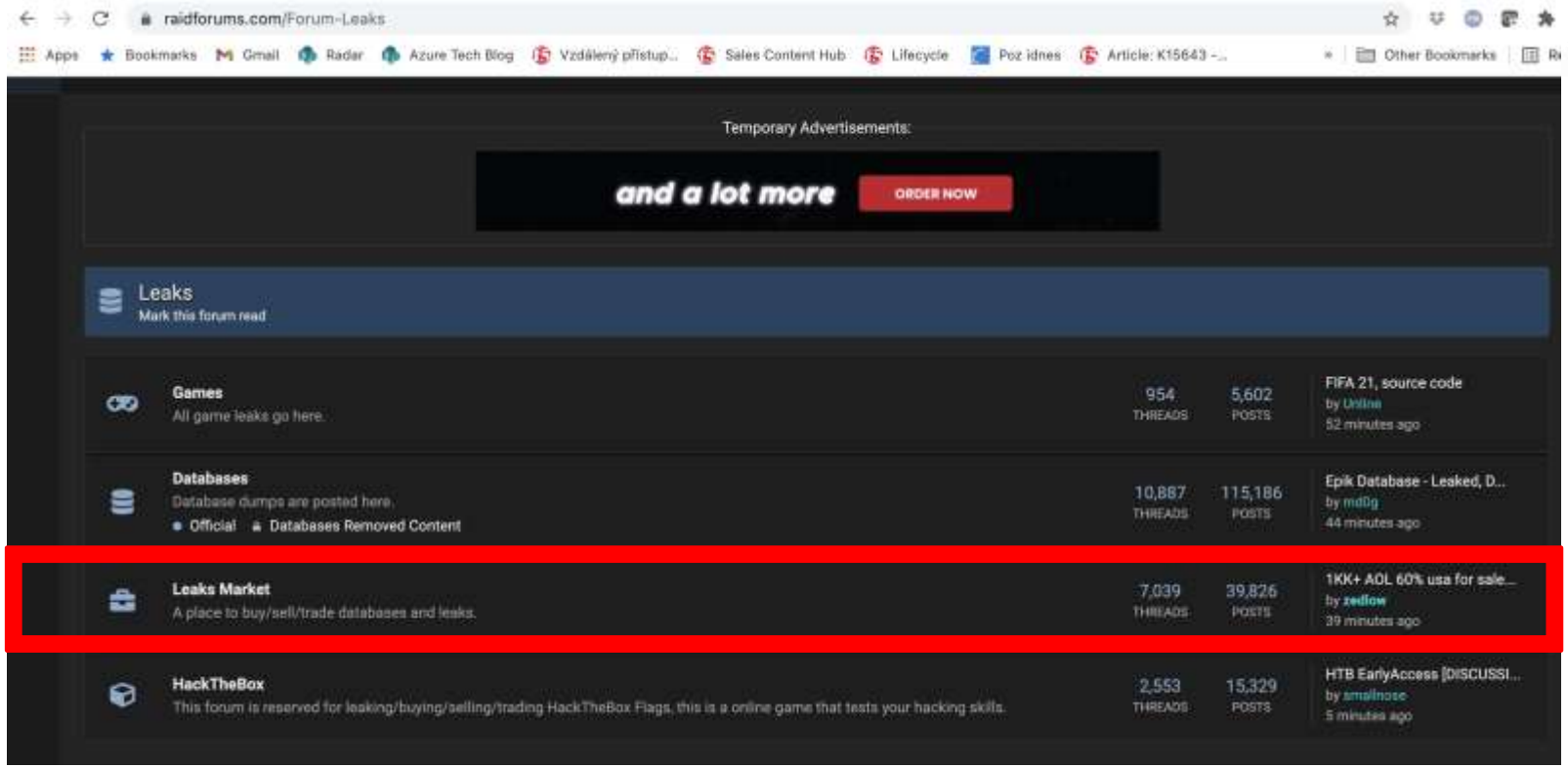
Vážený zákazníku,

Obdrželi jste novou důležitou zprávu.

Chcete-li si přečíst zprávu, přihlaste se do naší níže uvedené webové stránky.

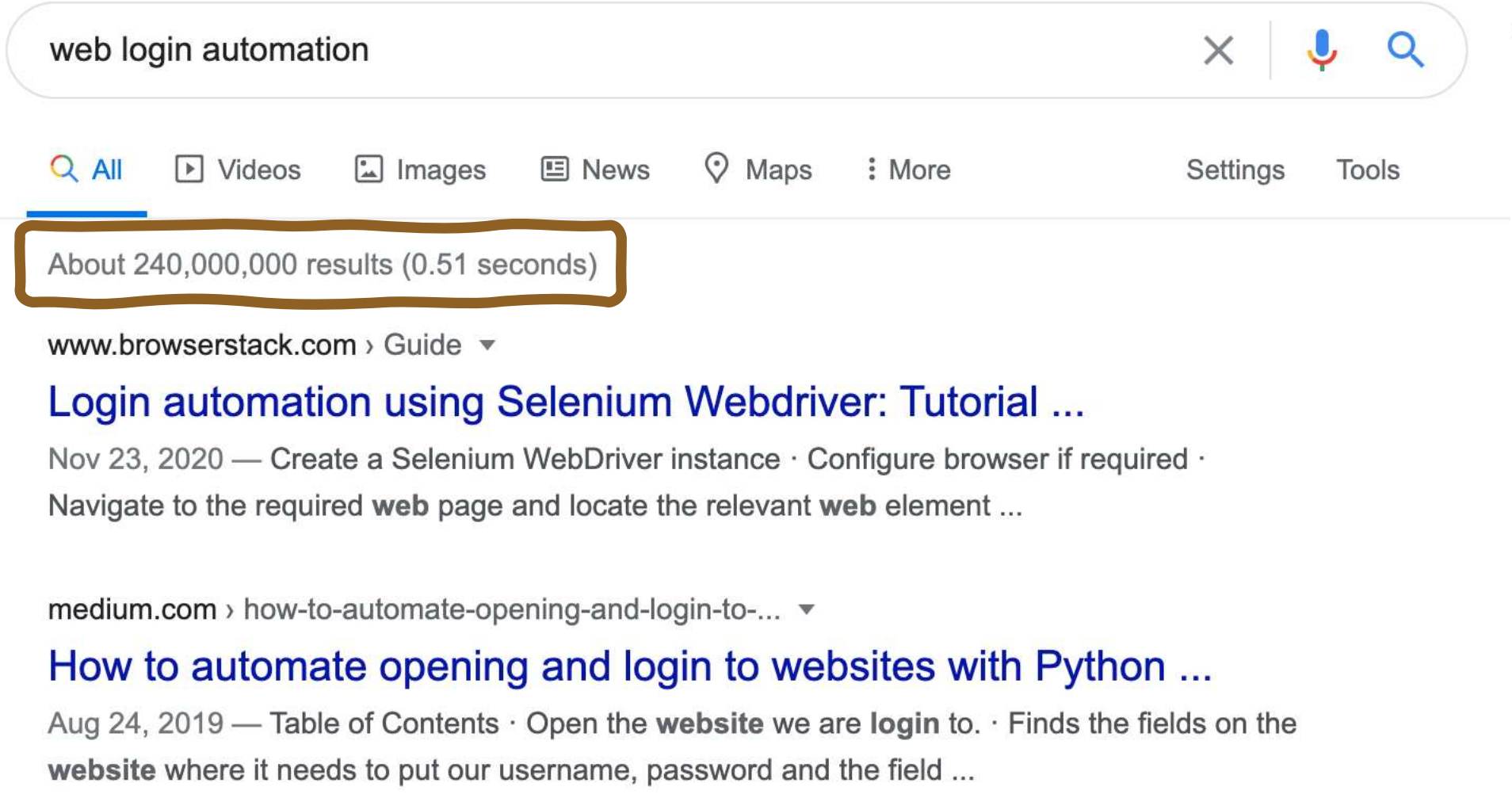
MALWARE ATTACKS

Credential Stuffing
Krok 1: Získání uživatelských jmen a hesel



Leaks Market
A place to buy/sell/trade databases and leaks.
7,039 THREADS
39,826 POSTS

Credential Stuffing
Krok 2: Automatizace loginu do účtů



Od jednoduchých skriptů…

curl://

No device or browser spoofing

No user interaction

IP Types

Countries

ASNs

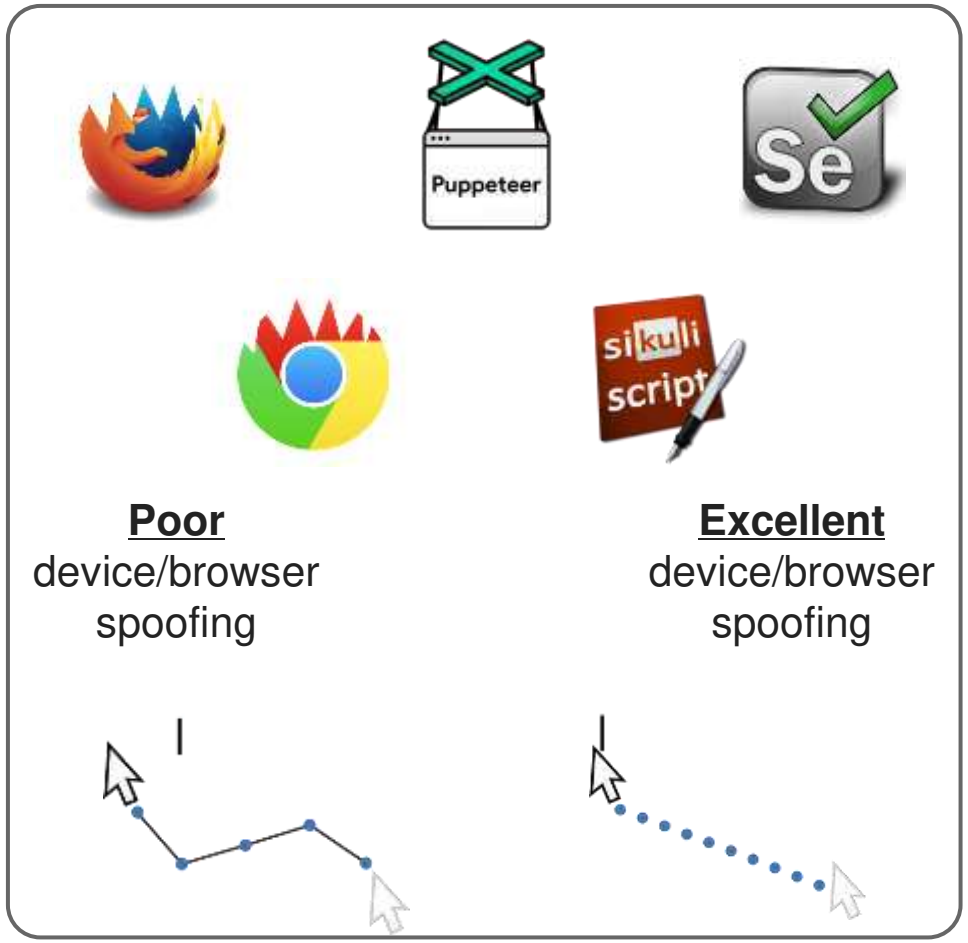
IPs

Přes sofistikované nástroje imitující lidské uživatele

curl://

No device or browser spoofing

No user interaction



IP Types

Countries

ASNs

IPs

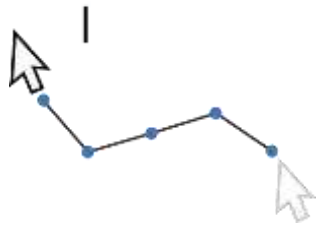
Až po lidské farmy provádějící spoofing zařízení a browserů

curl://

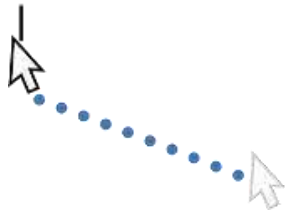
No device or browser spoofing

No user interaction

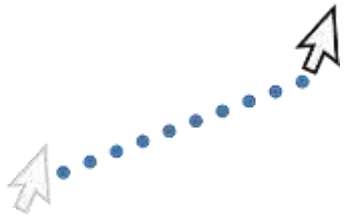
Poor device/browser spoofing



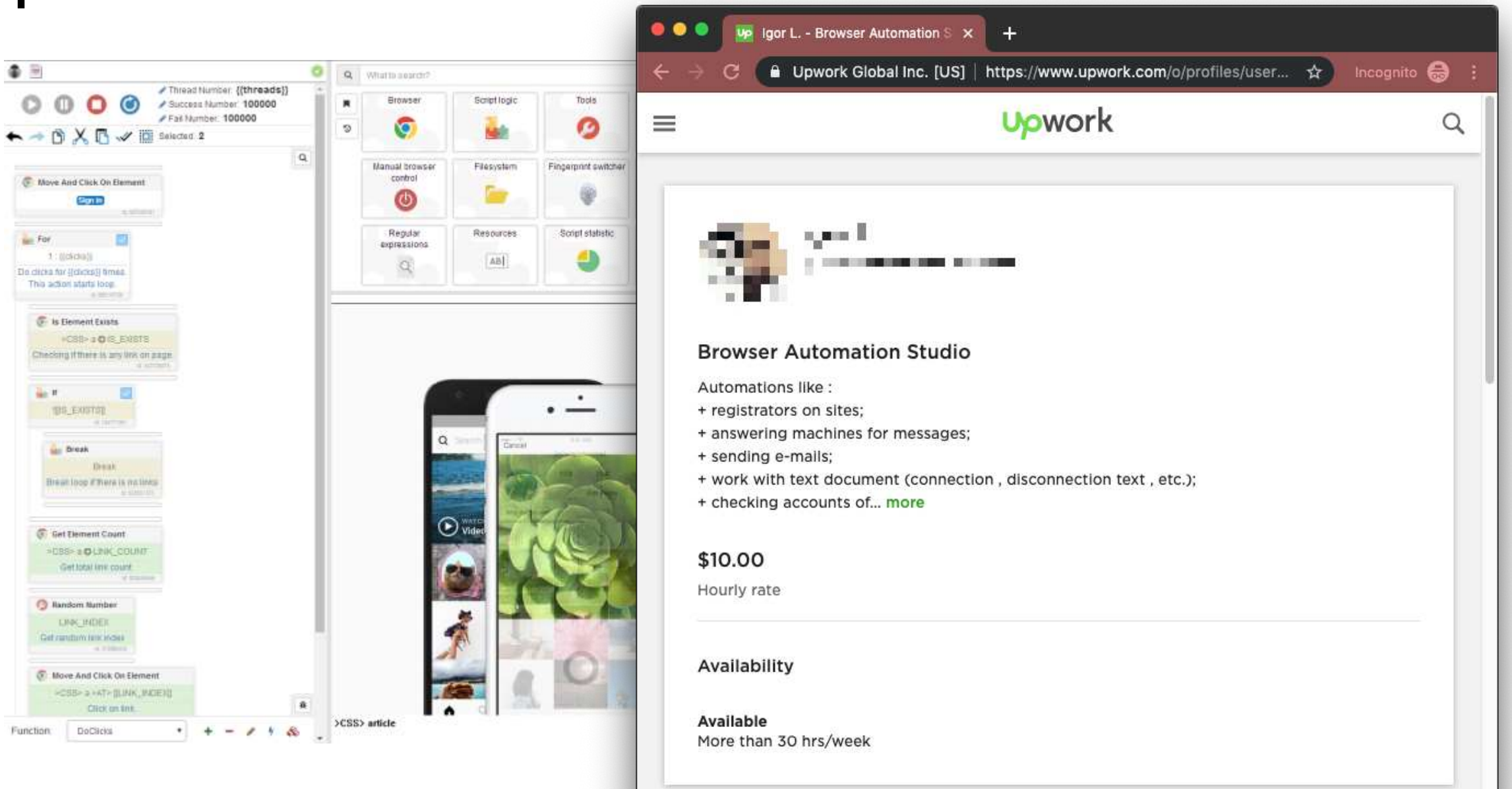
Excellent device/browser spoofing



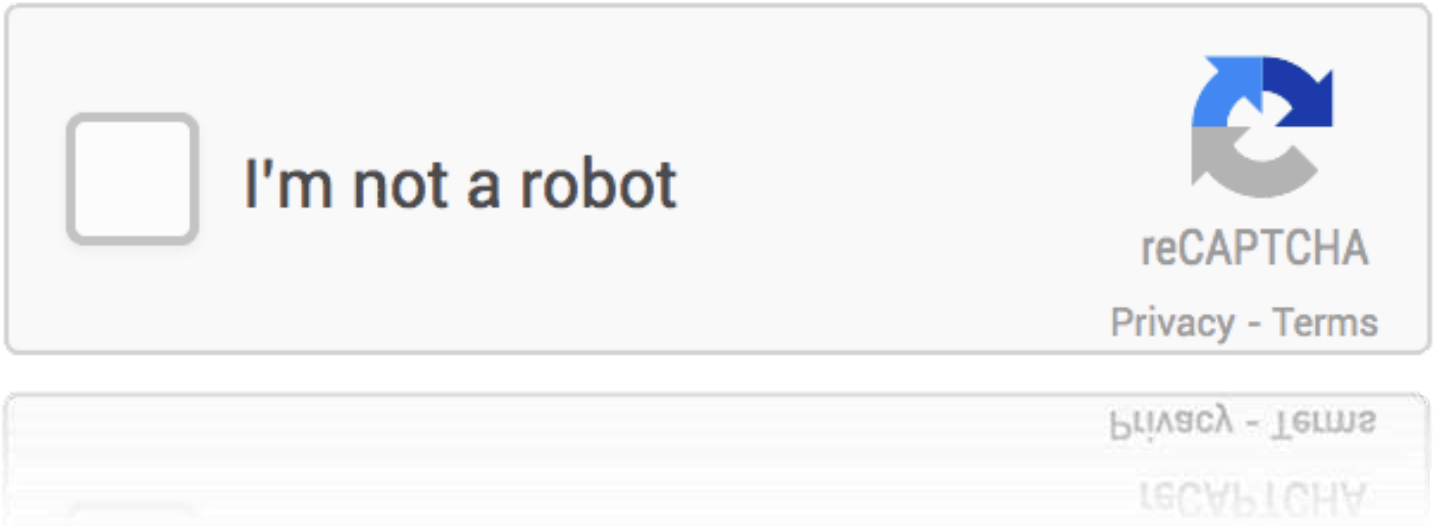
Real devices/browsers with some spoofing



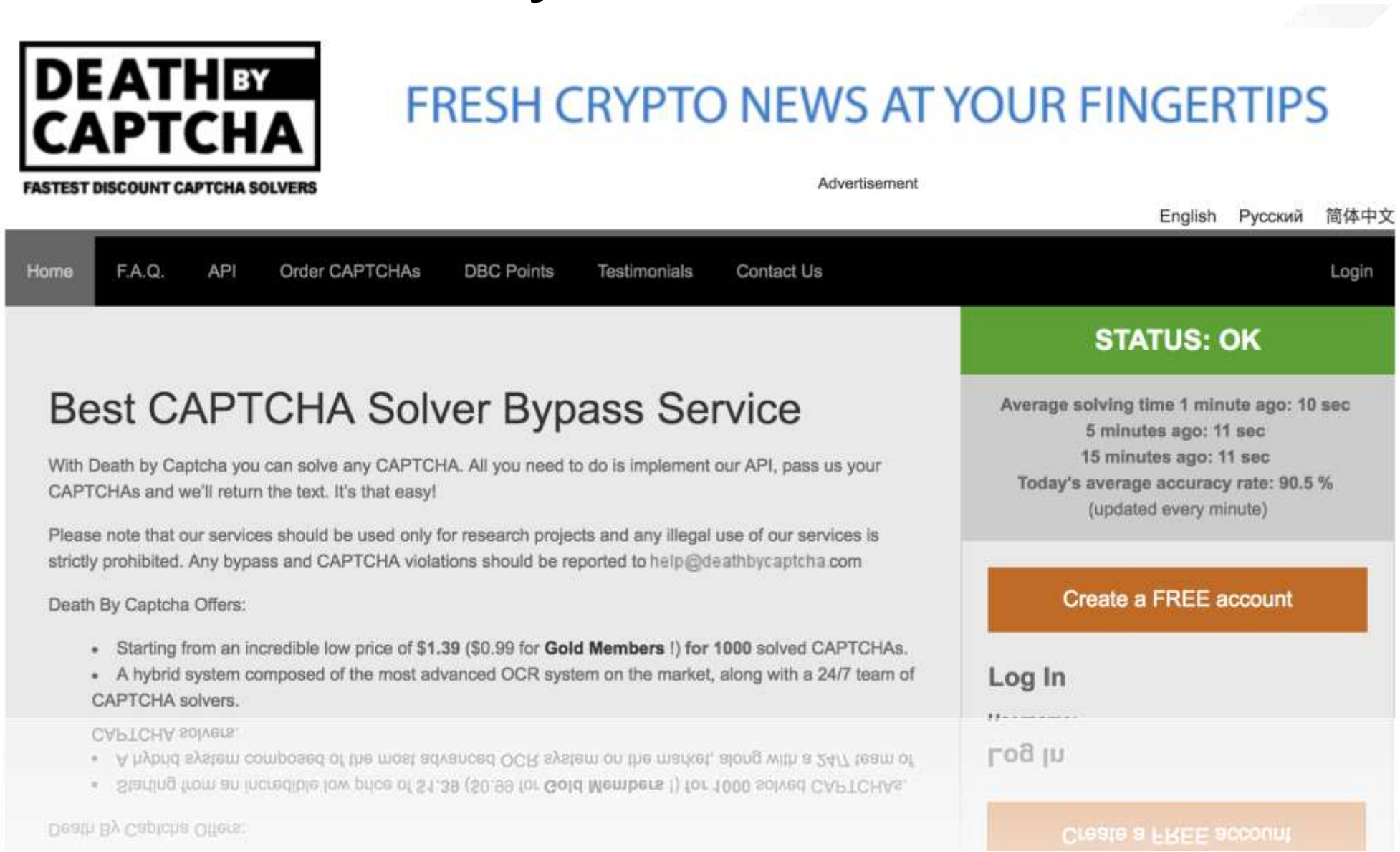
Nejste experti na Browser Automation Studio? Zaplat'te si specialistu on-line!



Credential Stuffing
Krok 3: Prolomení ochrany



Credential Stuffing
Krok 3: Prolomení ochrany



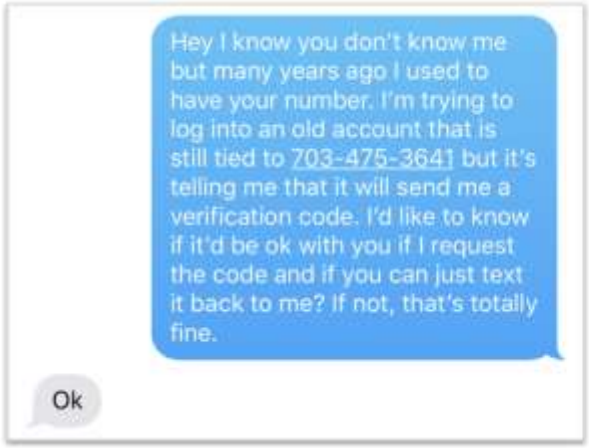
Credential Stuffing
Krok 3: Prolomení ochrany

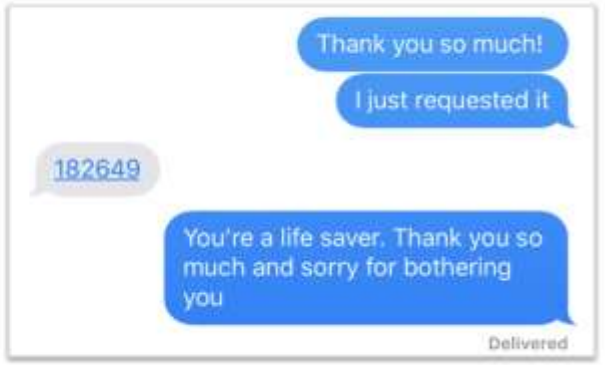
MFA nezastaví útoky credential stuffing

MFA zastaví automatizované ATO útoky

Jak útočníci obejdou MFA?

SOCIÁLNÍ INŽENÝRSTVÍ





POMOCÍ ZRANITELNOSTÍ V ÚSTŘEDNÁCH OPERÁTORA (SS7 PROTOKOL)

PHONE HACKING THROUGH SS7 IS FRIGHTENINGLY EASY AND EFFECTIVE

Aug 28, 2017 5:38:58 PM

Imagine a world in which a low-budget hackers can track your every move, listen to your calls, read your texts, drain your bank account, and so on. All of this without leaving their rooms, and from a continent away. Imagine no more. Due to vulnerabilities in the SS7 protocol, this is the world in which you live right now.

- A computer
- A Linux OS
- A software development kit for SS7

Source: https://blog.securegroup.com/phone-hacking-through-ss7-is-frighteningly-easy-and-effective

Pozor na podvodné telefonáty! Podvodníci se opět vydávají za zaměstnance banky nebo policisty a chtějí vás připravit o peníze.

26.5. 2021 | Vlna podvodných zpráv: Kontrolujte si, na co klikáte a co potvrzujete

Pozor na podvodné SMS zprávy a e-maily, pomocí kterých se podvodníci snaží vyzrát na zabezpečení internetového bankovnictví a ukrást nepozorným klientům peníze z účtu. Zjistěte, jaké finty používají i jak se bránit.

Vážení klienti,

chtěli bychom vás upozornit na další podvodné emaily, kterých se nyní objevuje více. Některým klientům Komerční banky přišly v nedávné době kromě emailů s podvodnou notifikací též emaily s výzvou k ověření a aktualizaci dat. Odkaz v tomto emailu vede na podvrženou přihlašovací obrazovku do internetového bankovnictví.

Hackers Steal Wealth of Data from Game Giant EA

The data includes source code for FIFA 21 and the Frostbite engine.

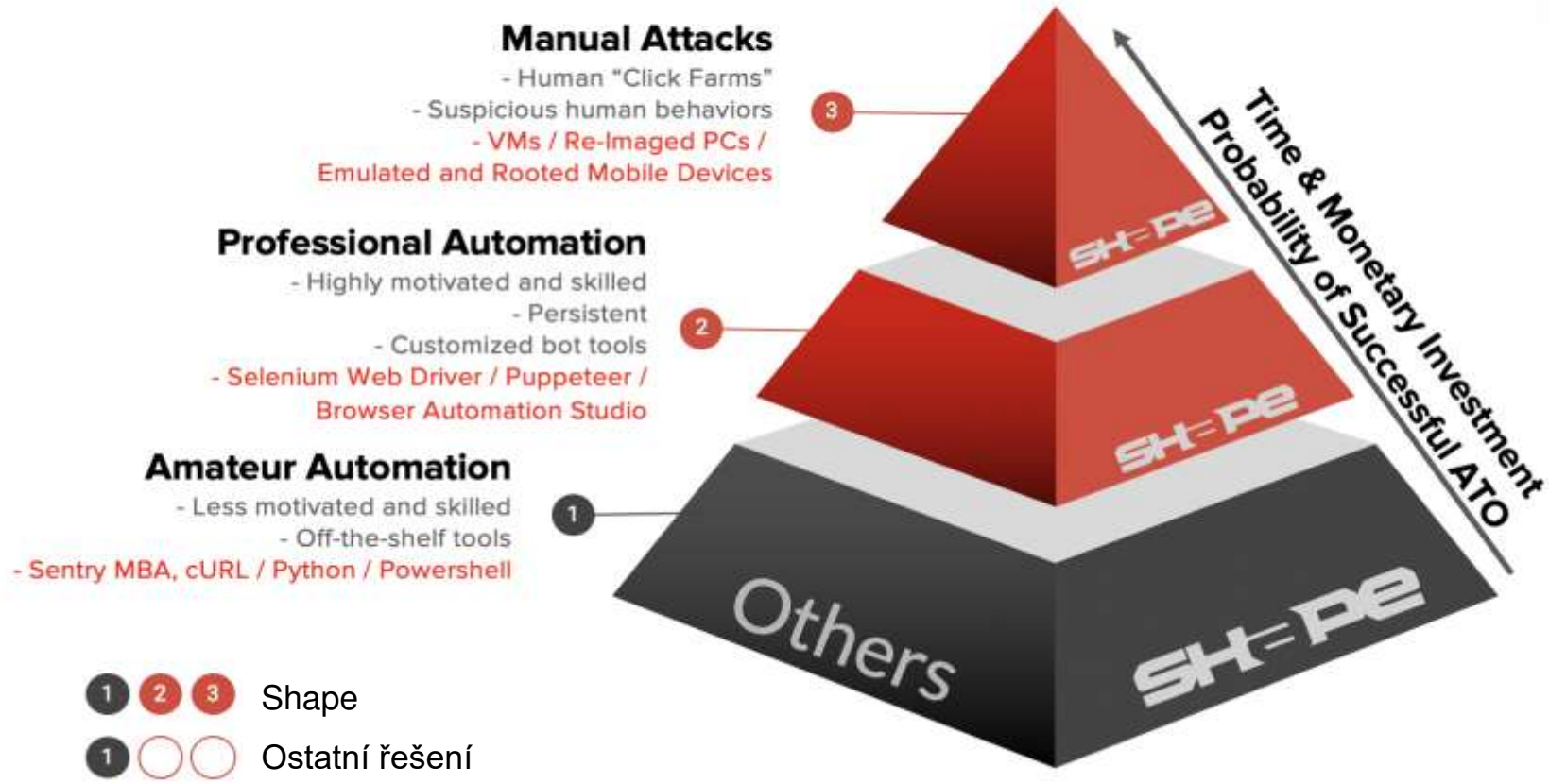
By Joseph Cox

June 10, 2021, 5:56pm Share Tweet Snap

Last week Motherboard revealed that hackers stole a wealth of data from game publishing giant Electronic Arts, including source code for the Frostbite engine and *FIFA* 21 game. The hackers said they did this, in part, by purchasing a cookie for $10 that let them log into an EA Slack account, and then tricking EA's IT support into granting access to the company's internal network.

Credential Stuffing
Krok 4: Distribuce pomocí botů

Ochrana pomocí Shape Security:
Struktura dnešních útoků & Evoluce chování útočníků



Shape analyzuje provoz a pomáhá odpovědět na tyto dotazy

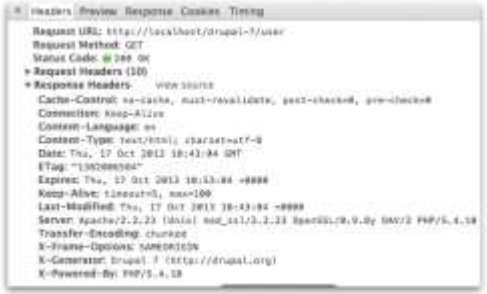
Jsi člověk?

Jsi dobrý nebo zlý?

Jsi ten, za koho se vydáváš?

Analýza signálů s velkou přesností odliší dobrý provoz od zlého

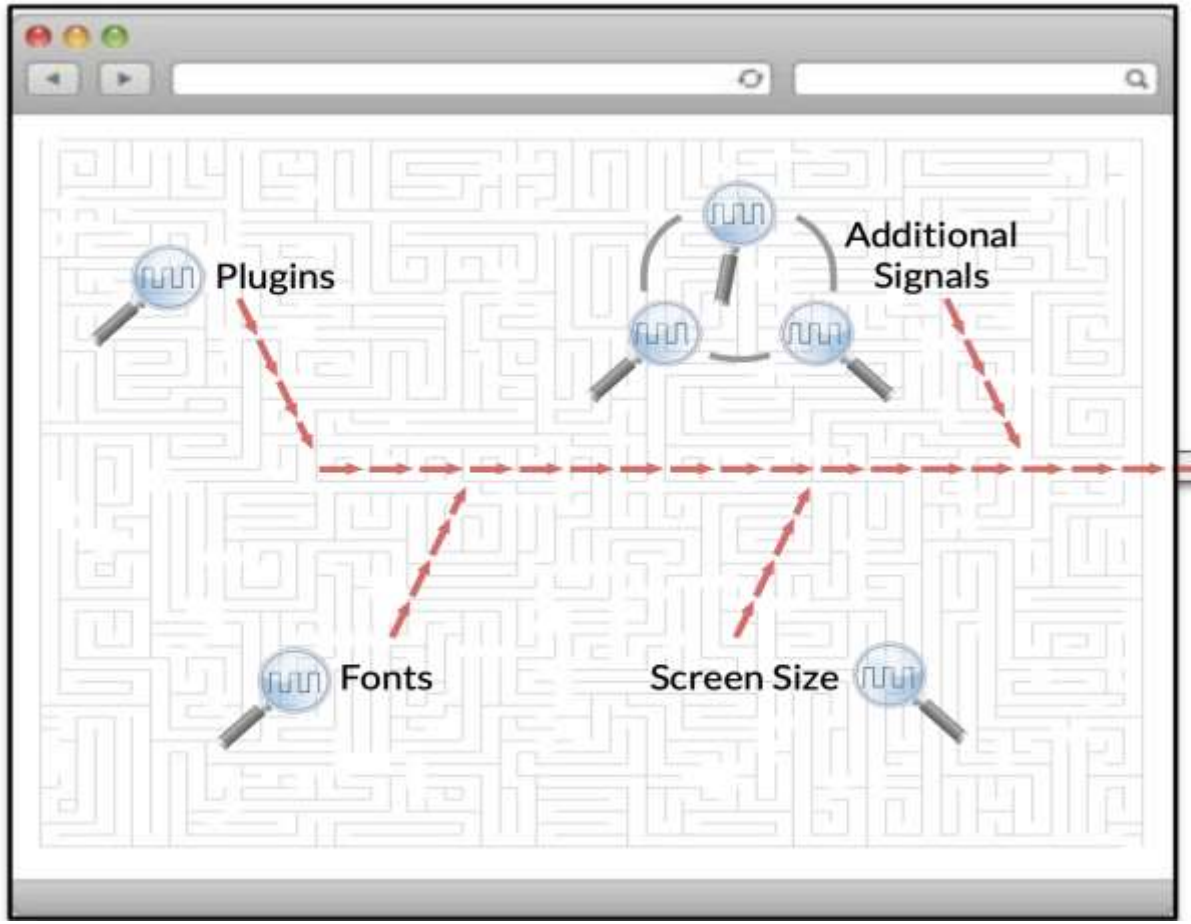
Zákaznický účet CO?



Síť JAK?

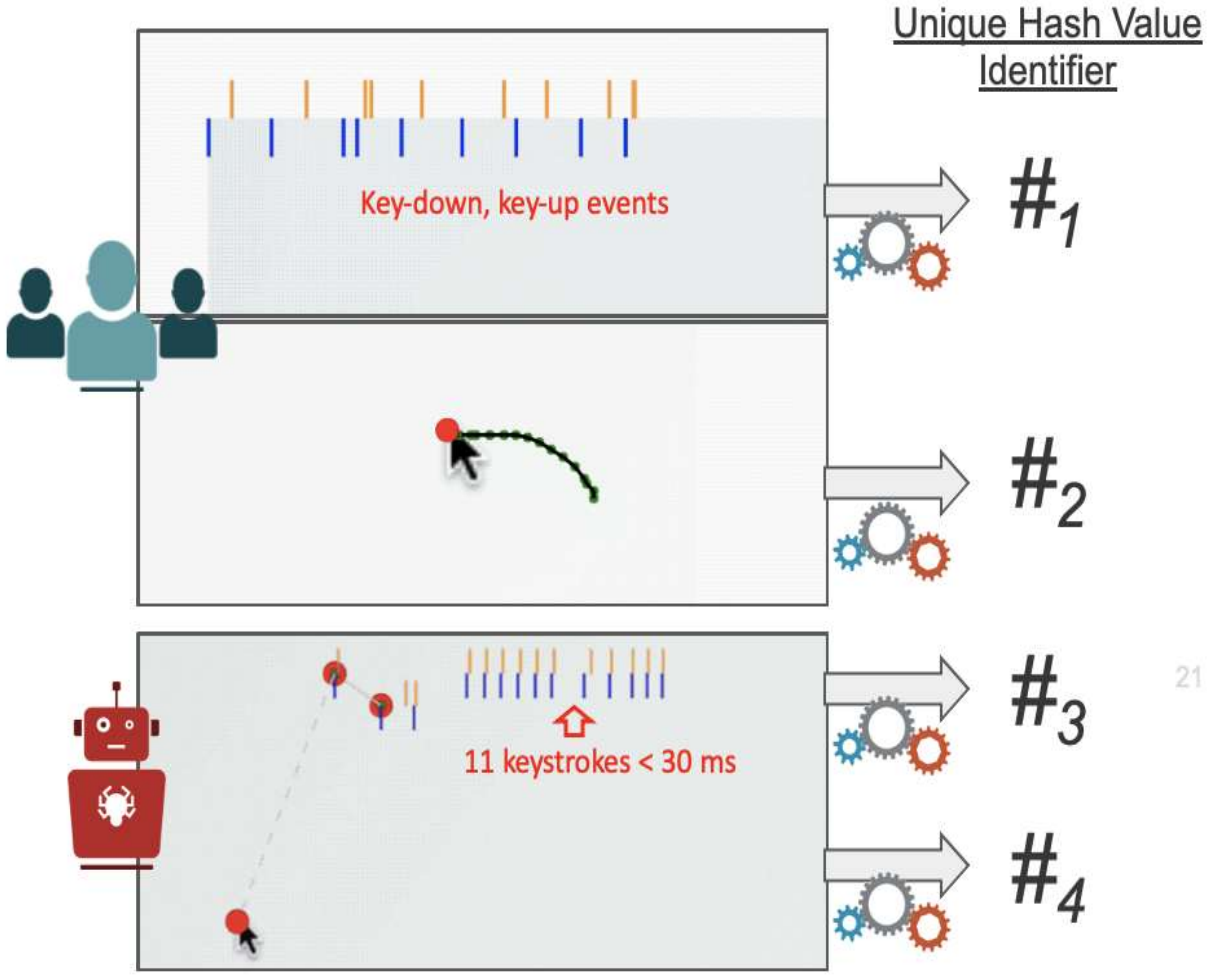
Chování uživatele KDO?

Shape používá technologii tvz. otisku prstu webového prohlížeče

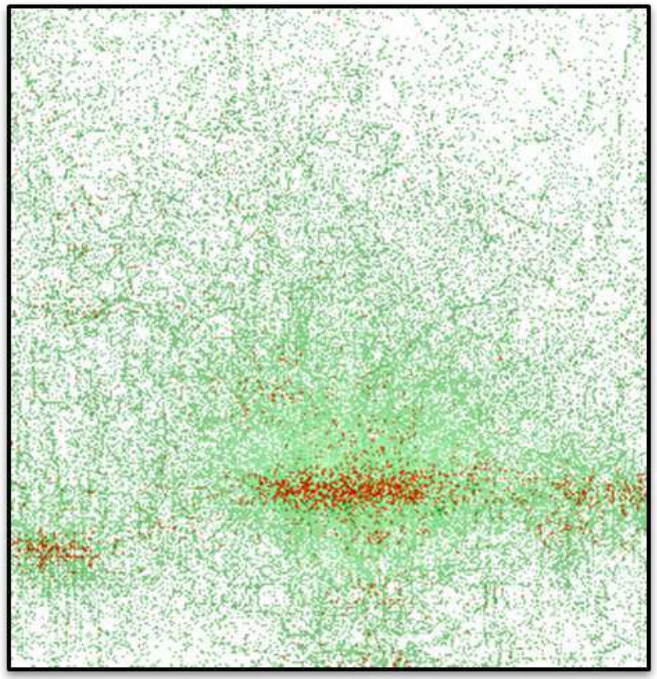


Signály chování uživatele sbírá Shape sbírá pomocí Java scriptu

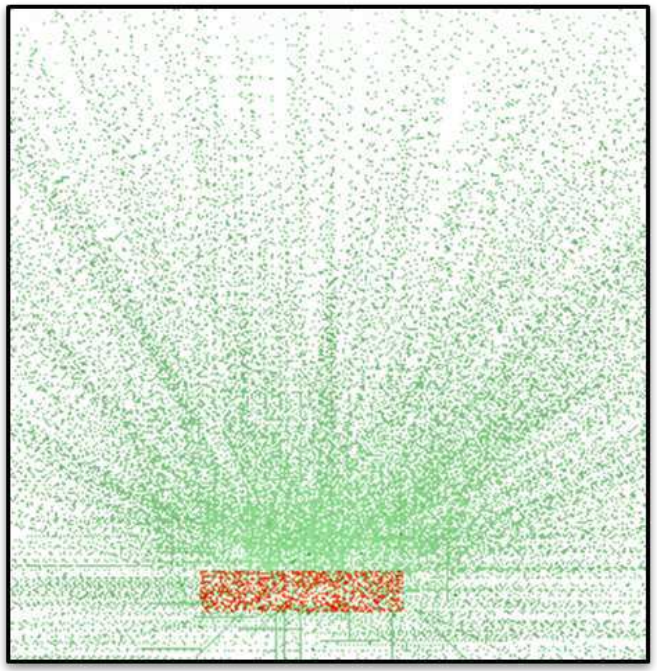
Blue Bar	Key-down.
Orange Bar	Key-up.
Red Circle	Mouse-click.
Green Tick	Captured mouse event.
Dashed Line	High speed movement between two points.
Brown Square	Long pause.
Grey Line	Transition from non-mouse event to mouse event.



Ukázka pohybu a klikání na myši běžného uživatele a automatu, které je Shape schopen rozpoznat



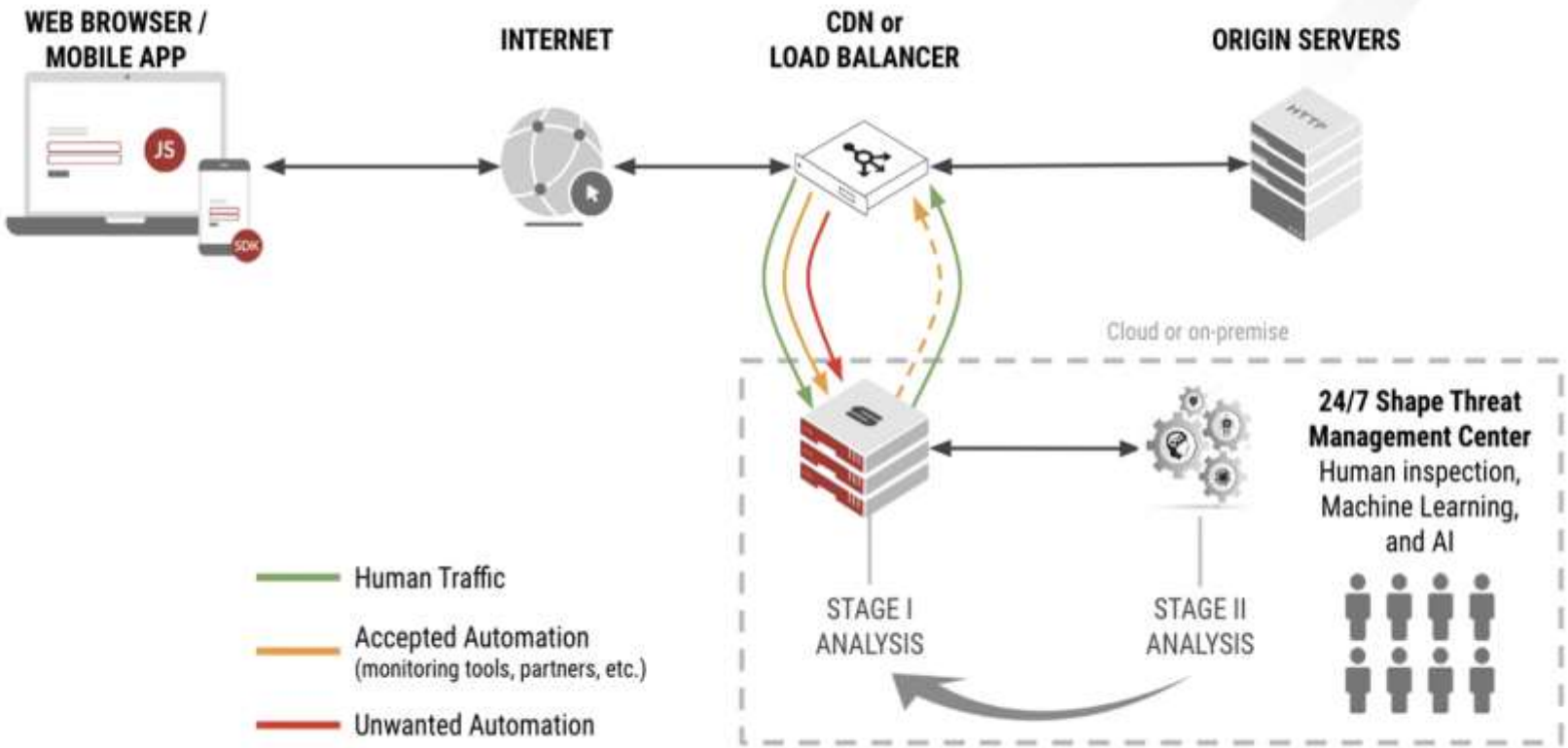
Legitimate Users



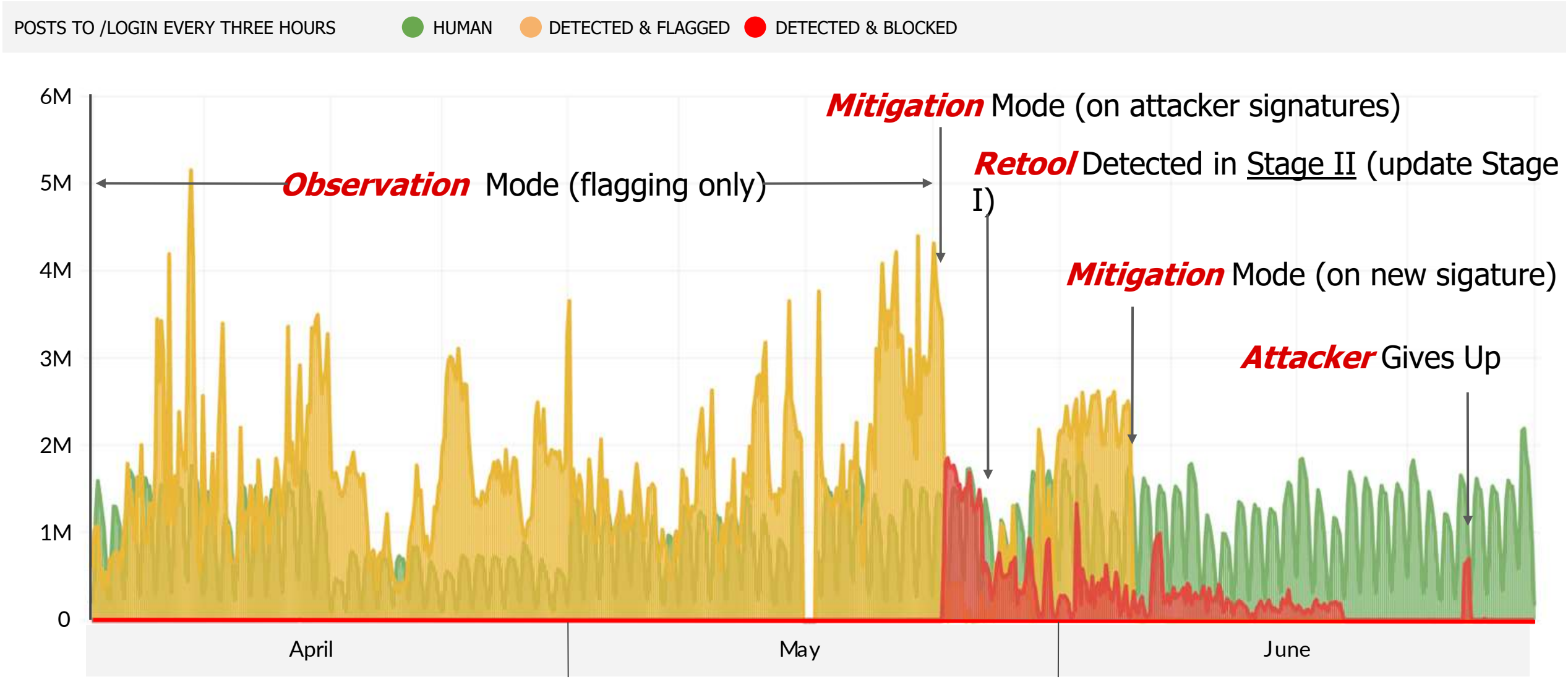
Bots

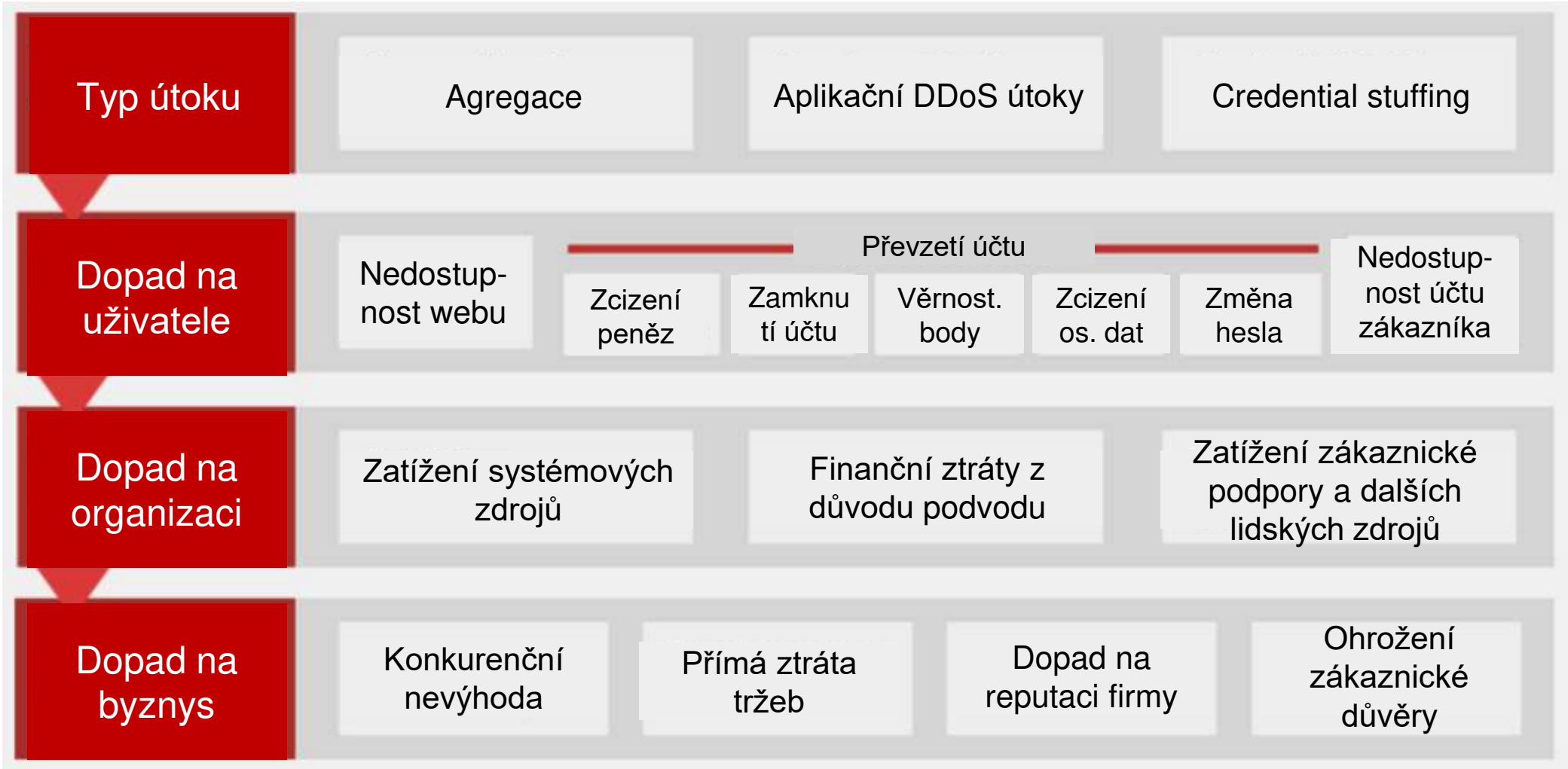
Mouse Move Mouse Click

Architektura nasazení technologie Shape



Příklad zákazníka chráněného pomocí Shape Security




Typ útoku
Agregace
Aplikační DDoS útoky
Credential stuffing
Dopad na uživatele
Nedostup-nost webu
Převzetí účtu
Zcizení peněz
Zamknutí účtu
Věrnost. body
Zcizení os. dat
Změna hesla
Nedostup-nost účtu zákazníka
Dopad na organizaci
Zatížení systémových zdrojů
Finanční ztráty z důvodu podvodu
Zatížení zákaznické podpory a dalších lidských zdrojů
Dopad na byznys
Konkurenční nevýhoda
Přímá ztráta tržeb
Dopad na reputaci firmy
Ohrožení zákaznické důvěry

Platforma Shape Security

Shape Defense

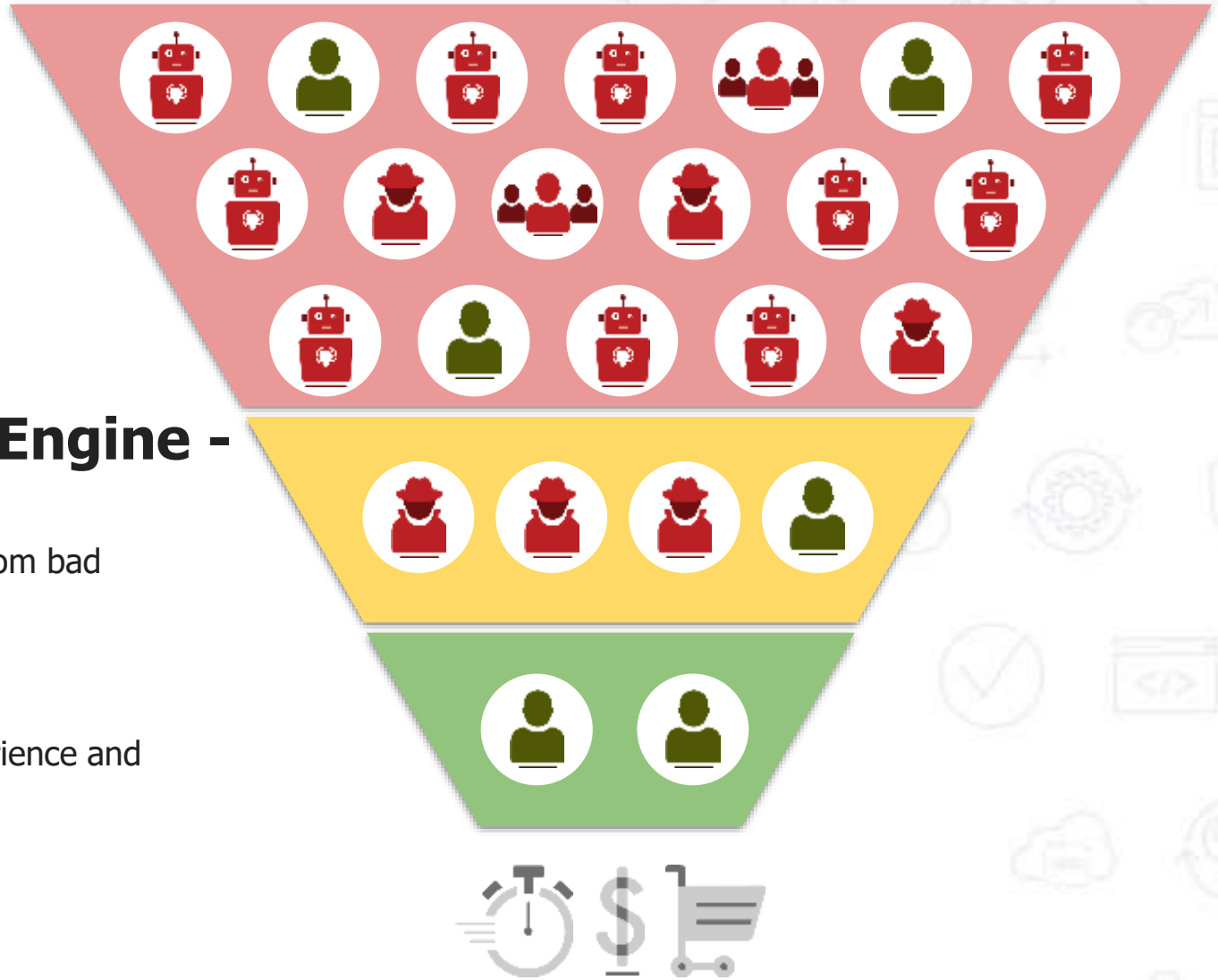
Identify and mitigate unwanted traffic

Shape AI Fraud Engine - SAFE

Differentiate good customers from bad customers

Recognize

Create a friction free user experience and increase revenue



Bots

Human Clickfarm

Fraudsters and Criminals

Good Customers

Shape chrání největší B2C podniky před web podvody a zneužitími od 2011

- **60%** of the NA Consumer banking
- **500 million** financial services accounts
- **9** of the **Top 15** US banks
- **5** of the **Top 10** US credit card issuers
- **3** of the **Top 5** Healthcare Providers

- **60%** of the airline industry
- **30%** of the hotel industry
- **300 million** frequent flyer accounts
- **5** of the **Top 10** global airlines
- **3** of the **Top 5** global hotel chains

- **40%** of all US in-store mobile payments
- **100 million** ecommerce accounts
- **5** of the **Top 10** global eComm companies
- **2** of the **Top 3** Wireless Carriers
- Payroll & Government (Federal and State)

WELLS FARGO

CHASE

jetBlue

Loblaw COMPANIES LIMITED

Peapod

BARNEYS NEW YORK

Shape Enterprise Defence

…je pro organizace aktivně působící v onlinu klíčové z těchto důvodů:

- Chrání proti webovým podvodům, zejména ATO
- Organizace získá přehled o struktuře provozu a útocích
- Eliminuje reputační riziko a náklady související s podvody.
- Umožňuje nenápadně zabránit nežádoucí a povolit nechtěnou automatizaci