



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



SKUPINA ČEZ

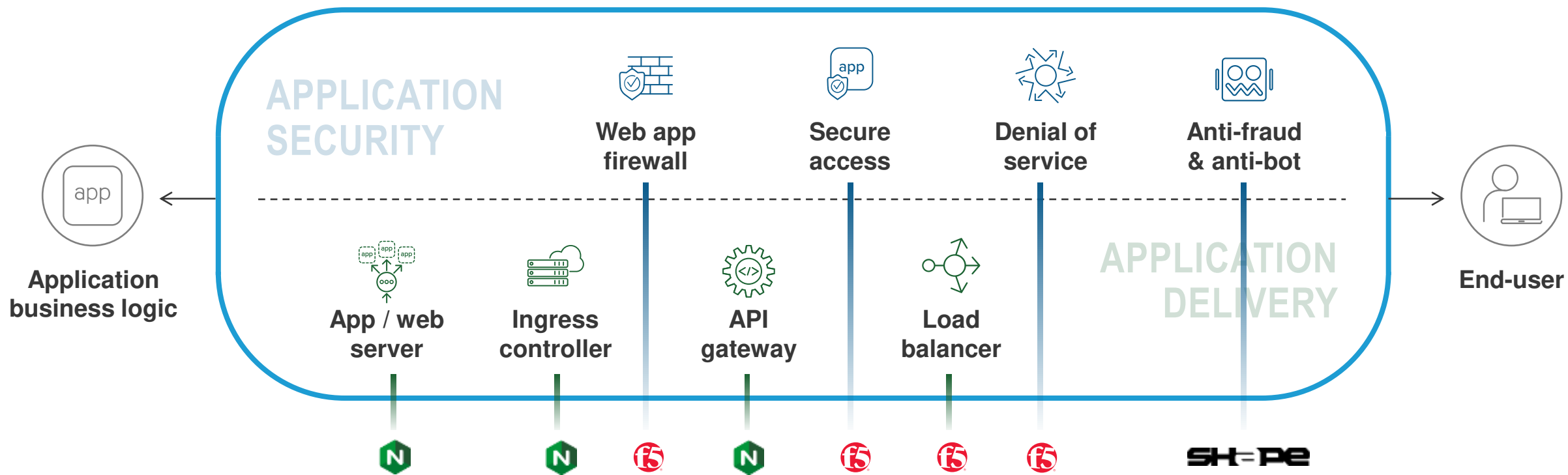


SPCSS

Státní pokladna
Centrum sdílených služeb

Správa informačních
technologií 

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



SHAPE / SILVERLINE

Secure and app insight anywhere



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



Tato zpráva vypadá nebezpečně



Obsahuje podezřelý odkaz, který byl v minulosti použit k odcizení osobních údajů. Neklikajte na odkazy ani v odpovědi neuvádějte osobní údaje.

Vážený zákazníku,

Obdrželi jste novou důležitou zprávu.

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

MALWARE ATTACKS

[078B1316-69BD0800-4CE22030-
CEE29414-7160049C](#)



✉ 0 📌 7 💎 0 = 7

Skype

Netflix

...known 2

GB

5.148...

±.00

0.70

Windows 7 Home
Premium



2019-04-12 14:08:14

2019-04-12 14:59:24

my.freecycle.org
login003.entiretec.com

accounts.mail.blueyonder.co.uk
www.itv.com ...other 5

Credential Stuffing

Krok 1: Získání uživatelských jmen a hesel

Temporary Advertisements:

and a lot more [ORDER NOW](#)

Leaks
Mark this forum read

Category	Description	Threads	Posts	Latest Post
Games	All game leaks go here.	954	5,602	FIFA 21, source code by Unlma 52 minutes ago
Databases	Database dumps are posted here. • Official • Databases Removed Content	10,887	115,186	Epik Database - Leaked, D... by midig 44 minutes ago
Leaks Market	A place to buy/sell/trade databases and leaks.	7,039	39,826	1KK+ AOL 60% usa for sale... by redlow 39 minutes ago
HackTheBox	This forum is reserved for leaking/buying/selling/trading HackTheBox Flags, this is a online game that tests your hacking skills.	2,553	15,329	HTB EarlyAccess [DISCUSSI... by smallnose 5 minutes ago



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

web login automation



All



Videos



Images



News



Maps



More

Settings

Tools

About 240,000,000 results (0.51 seconds)

www.browserstack.com › Guide ▾

Login automation using Selenium Webdriver: Tutorial ...


Nov 23, 2020 — Create a Selenium WebDriver instance · Configure browser if required · Navigate to the required **web** page and locate the relevant **web** element ...

medium.com › how-to-automate-opening-and-login-to-... ▾

How to automate opening and login to websites with Python ...

Aug 24, 2019 — Table of Contents · Open the **website** we are **login** to. · Finds the fields on the **website** where it needs to put our username, password and the field ...

Od jednoduchých skriptů...



MBA

curl://

No device or
browser spoofing

No user
interaction



IP Types

Countries

ASNs

IPs

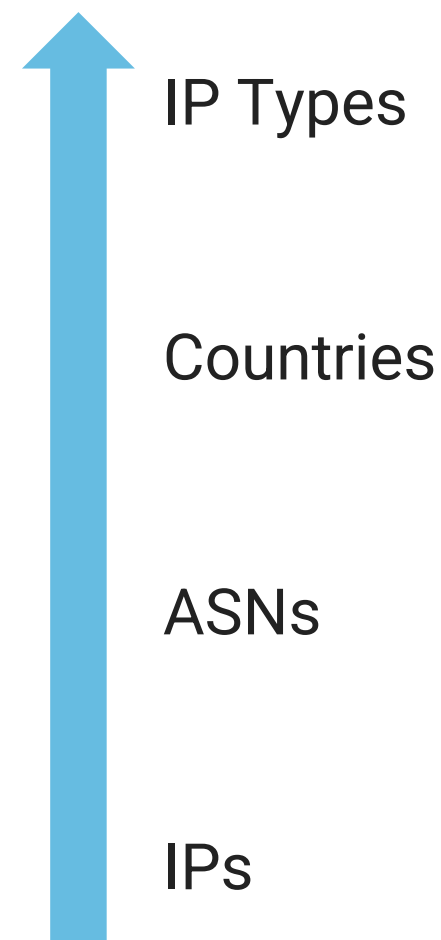
Přes sofistikované nástroje imitující lidské uživatele



curl://

No device or browser spoofing

No user interaction



Až po lidské farmy provádějící spoofing zařízení a browserů



curl://

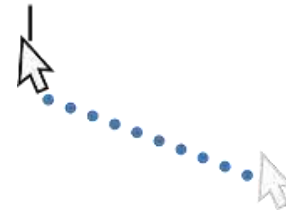
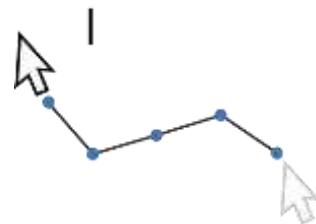
No device or browser spoofing

No user interaction

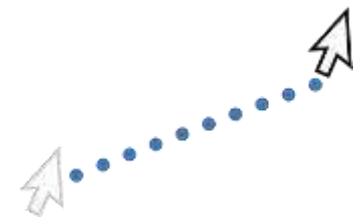


Poor device/browser spoofing

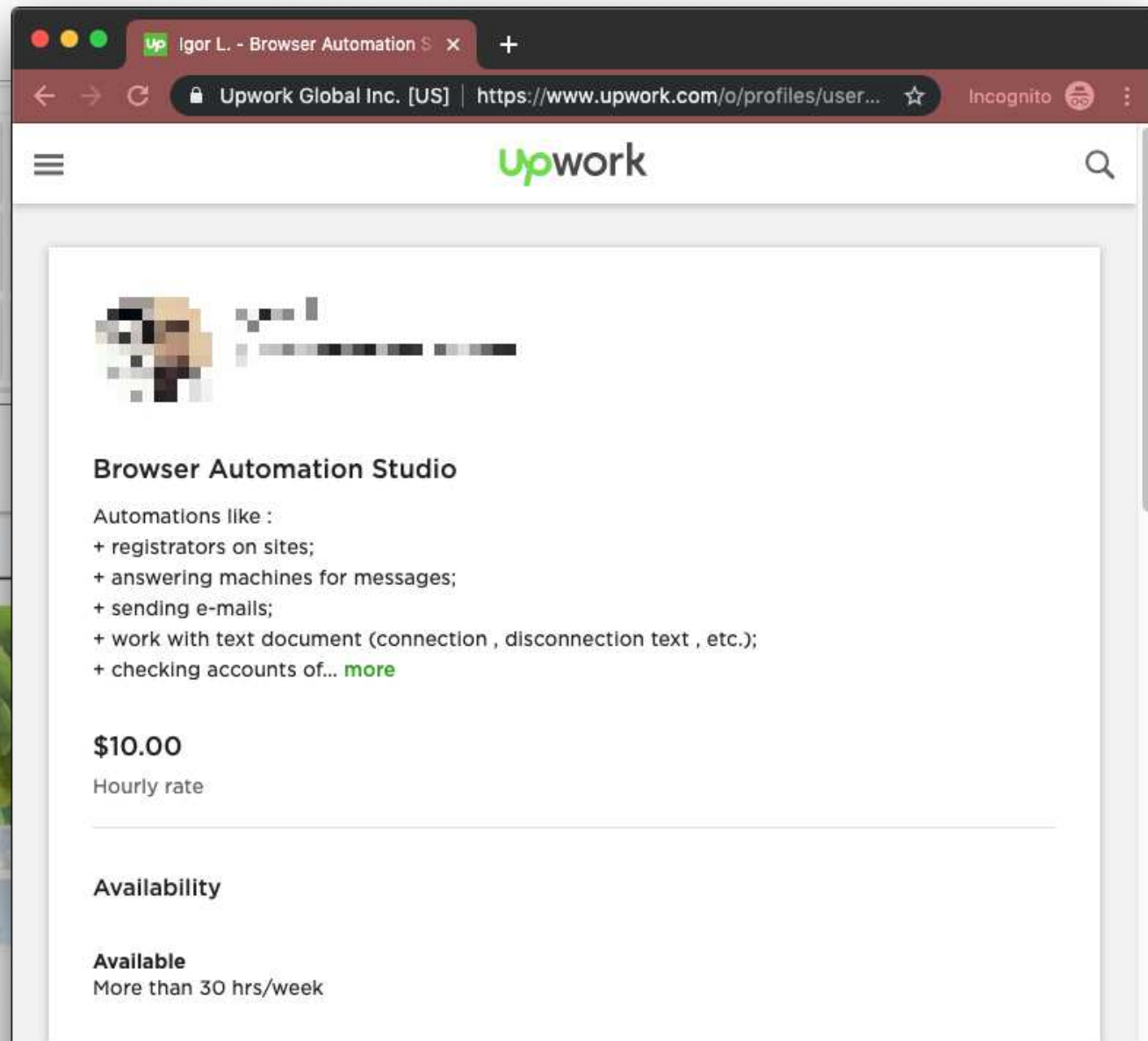
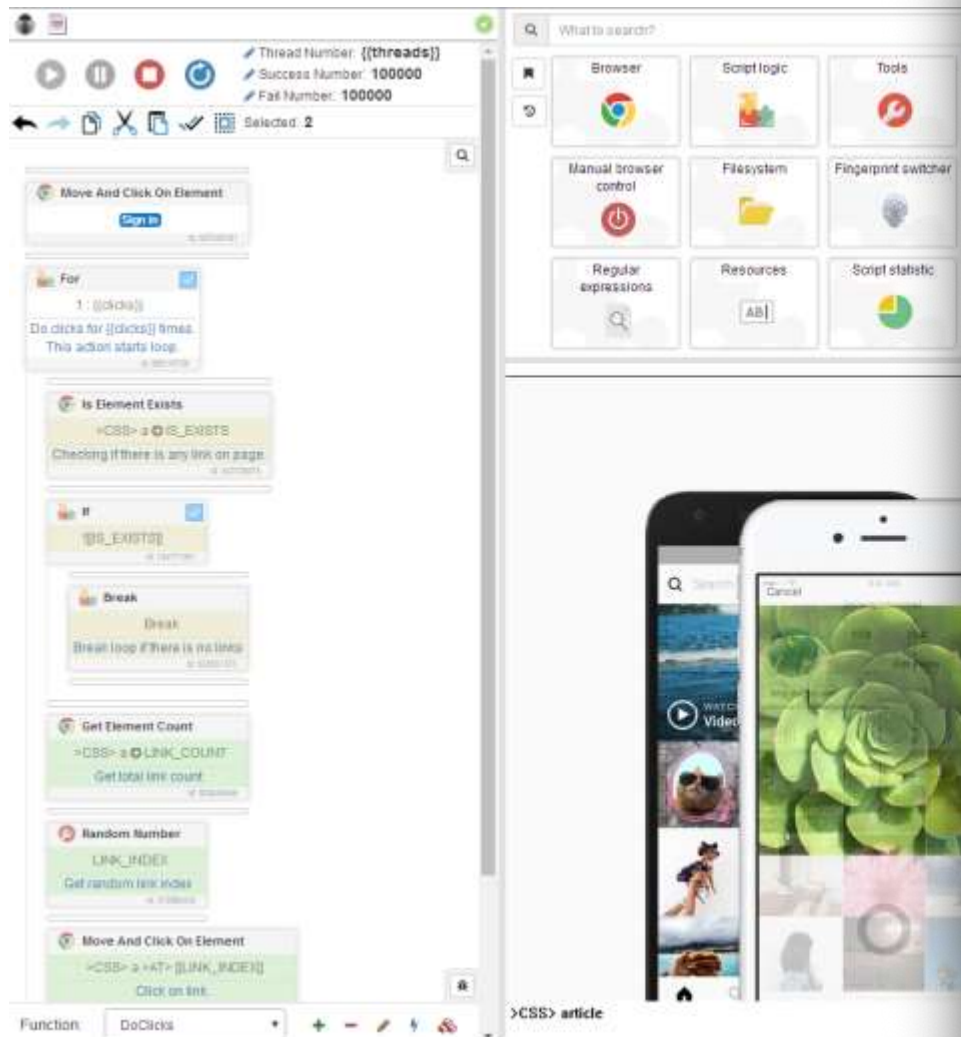
Excellent device/browser spoofing



Real devices/browsers with some spoofing

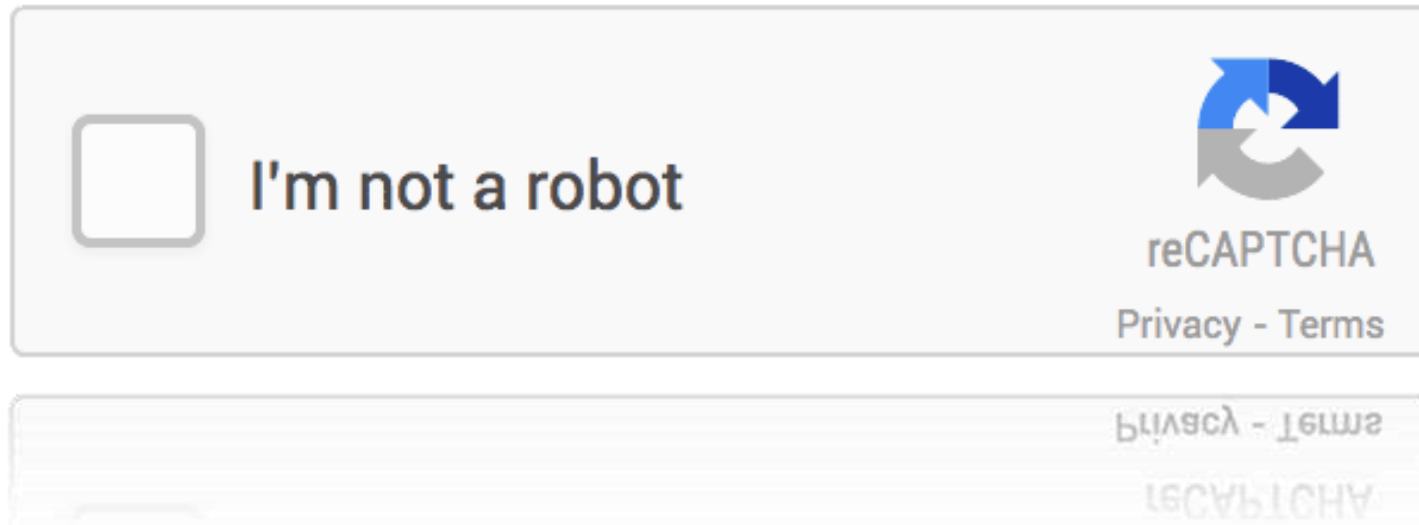


Nejste experti na Browser Automation Studio? Zaplat'te si specialistu on-line!



Credential Stuffing

Krok 3: Prolomení ochrany



Credential Stuffing

Krok 3: Prolomení ochrany



FRESH CRYPTO NEWS AT YOUR FINGERTIPS

Advertisement

English Русский 简体中文

Home F.A.Q. API Order CAPTCHAs DBC Points Testimonials Contact Us

Login

STATUS: OK

Best CAPTCHA Solver Bypass Service

With Death by Captcha you can solve any CAPTCHA. All you need to do is implement our API, pass us your CAPTCHAs and we'll return the text. It's that easy!

Please note that our services should be used only for research projects and any illegal use of our services is strictly prohibited. Any bypass and CAPTCHA violations should be reported to help@deathbycaptcha.com.

Death By Captcha Offers:

- Starting from an incredible low price of **\$1.39** (\$0.99 for **Gold Members** !) for **1000** solved CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.

CAPTCHA solvers:

- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.
- Starting from an incredible low price of **\$1.39** (\$0.99 for **Gold Members** !) for **1000** solved CAPTCHAs.

Death By Captcha Offers:

Average solving time 1 minute ago: 10 sec
5 minutes ago: 11 sec
15 minutes ago: 11 sec
Today's average accuracy rate: 90.5 %
(updated every minute)

Create a **FREE** account

Log In

Log In

Create a **FREE** account

Credential Stuffing

Krok 3: Prolomení ochrany

MFA nezastaví útoky credential stuffing
MFA zastaví automatizované ATO útoky

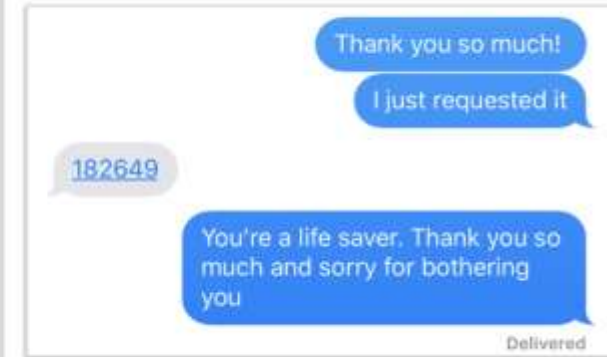
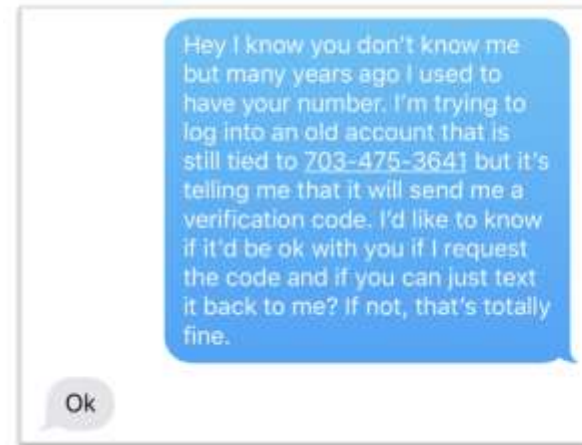
Jak útočníci obejdou MFA?

SOCIÁLNÍ INŽENÝRSTVÍ

Username
victim@gmail.com

Password

Submit



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 bankovníctví 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 bankovníctví.

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](#)

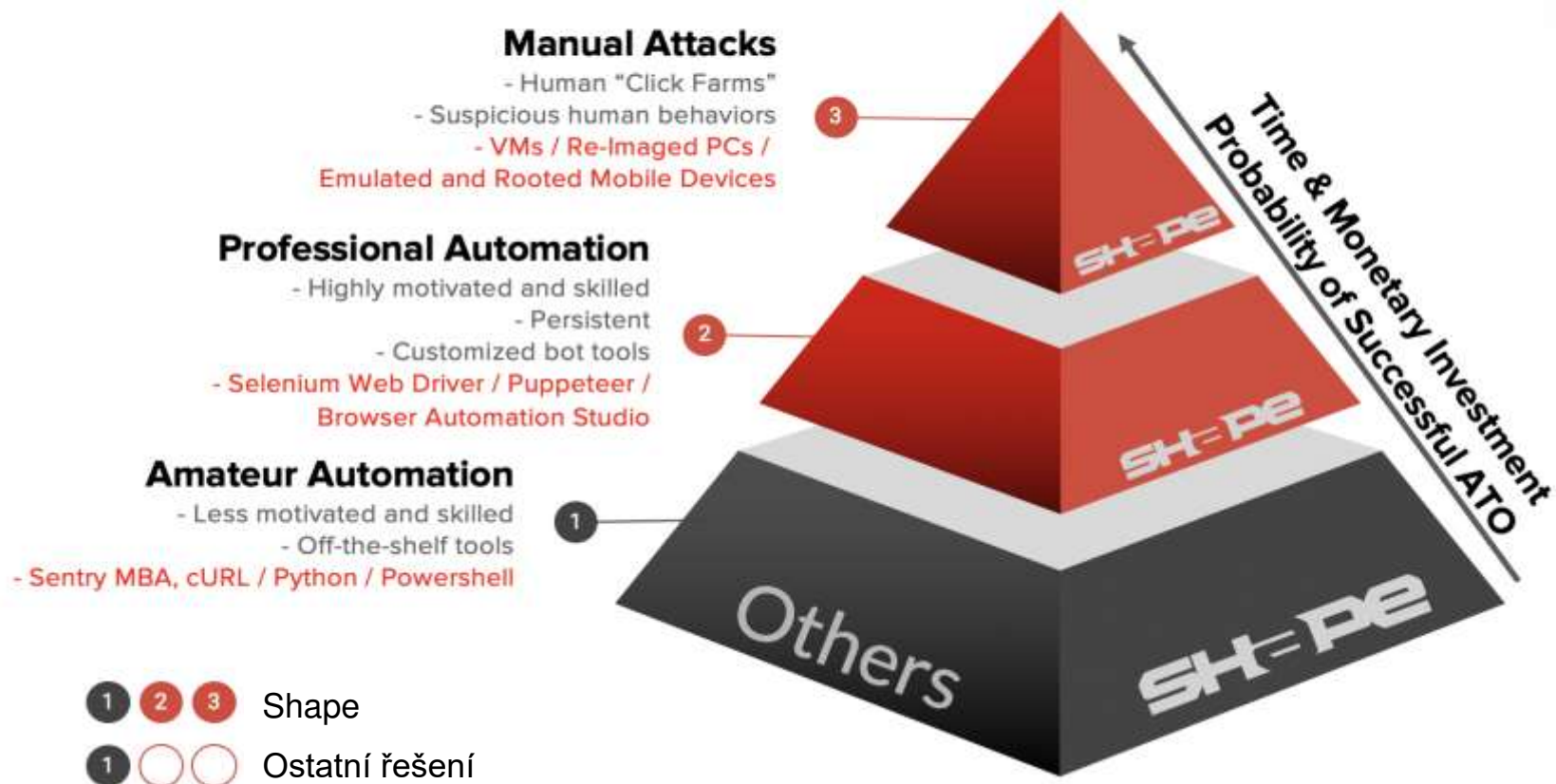
Last week [Motherboard](#) revealed that [hackers stole a wealth of data](#) from game publishing giant Electronic Arts, including source code for the Frostbite engine and FIFA 21 game. The hackers said they did this, in part, by purchasing a cookie for \$10 that let them [log into an EA Slack account](#), 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
človek?**

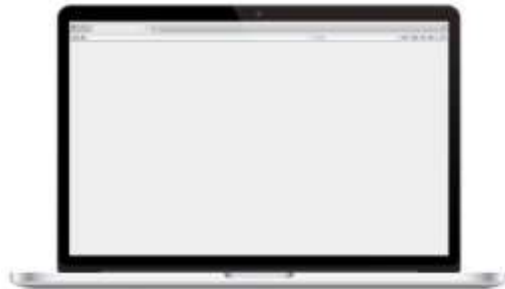


**Jsi dobrý
nebo zlý?**

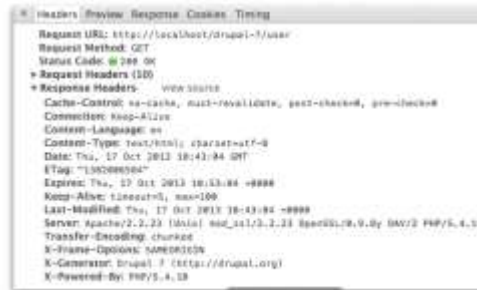


**Jsi ten, za
koho se
vydáváš?**

Analýza signálů s velkou přesností odliší dobrý provoz od zlého



**Zákaznický
účet
CO?**

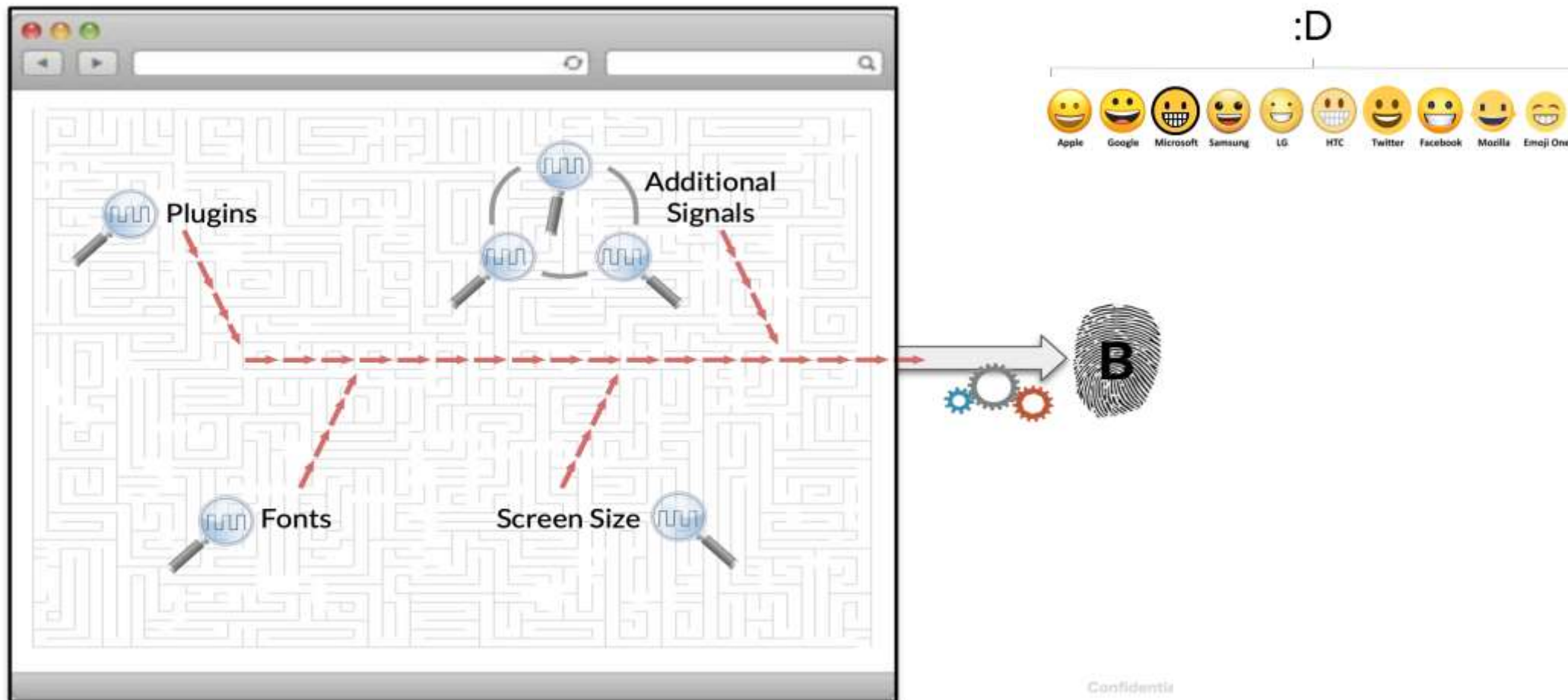


**Sít'
JAK?**



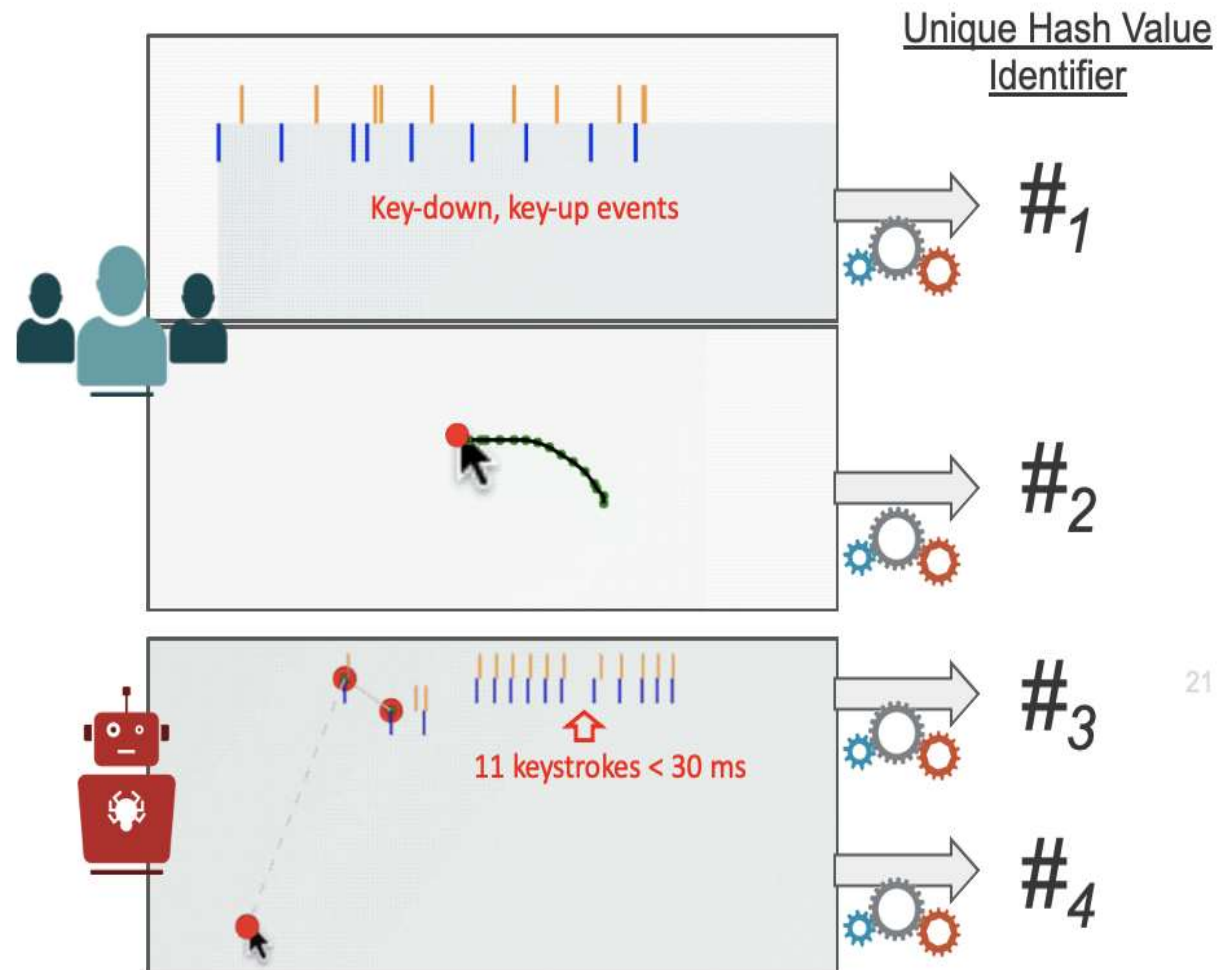
**Chování
uživatele
KDO?**

Shape používá technologii tzv. otisku prstu webového prohlížeče

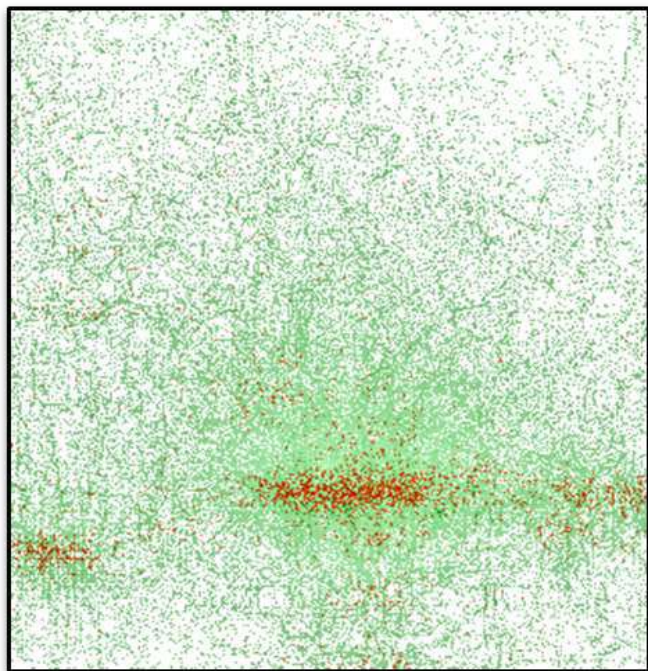


Signály chování uživatele sbírá Shape sbírá pomocí Java scriptu

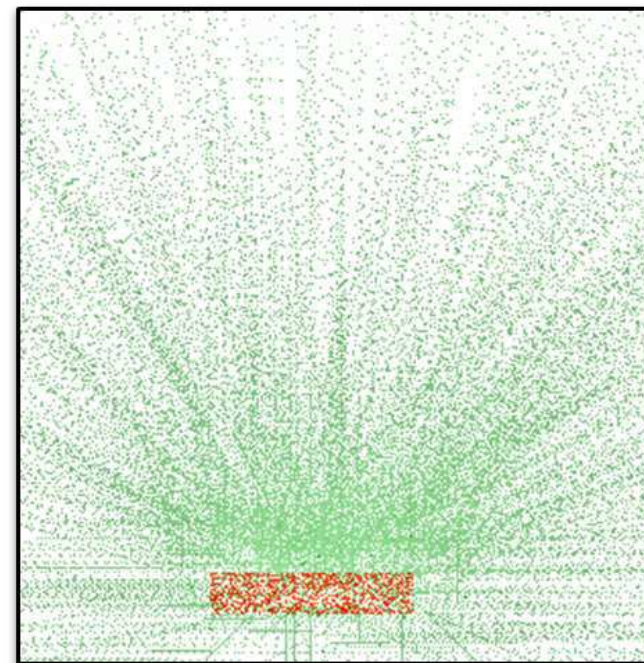
Blue Bar	Key-down.
Orange Bar	Key-up.
Red Circle	Mouse-click.
Green Tick	Captured mouse event.
Dashed Line	High speed movement between two points.
Brown Square	Long pause.
Grey Line	Transition from non-mouse event to mouse event.



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



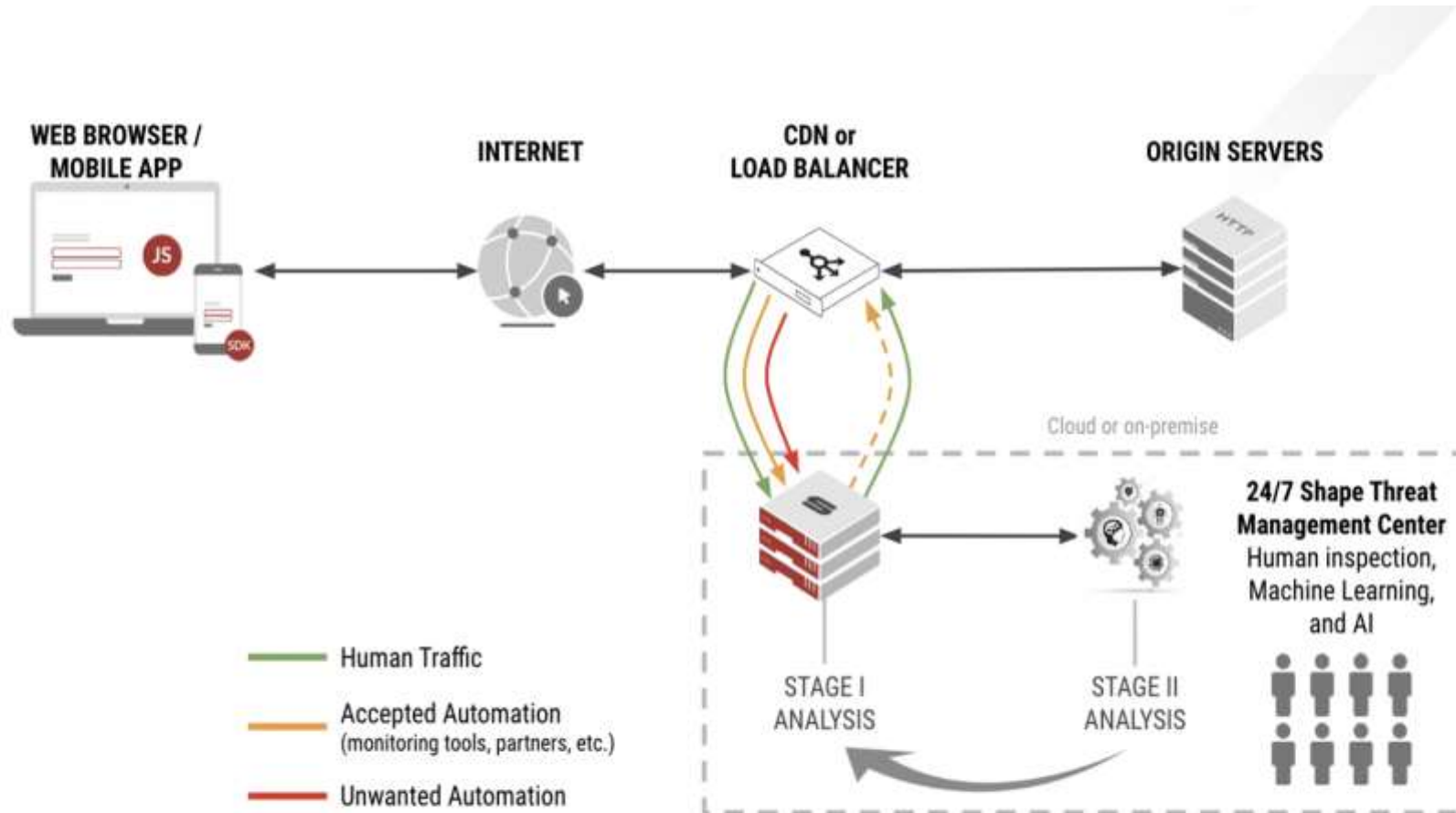
Legitimate Users



Bots

● Mouse Move ● Mouse Click

Architektura nasazení technologie Shape



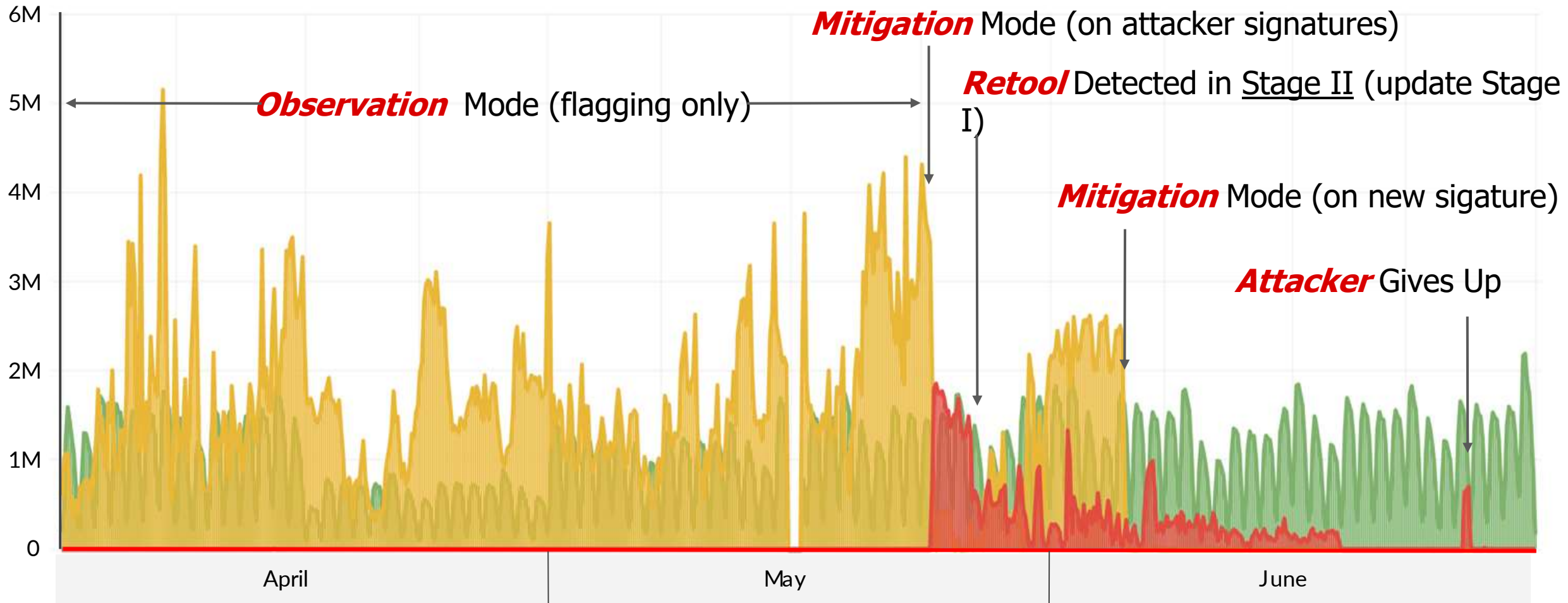
Příklad zákazníka chráněného pomocí Shape Security

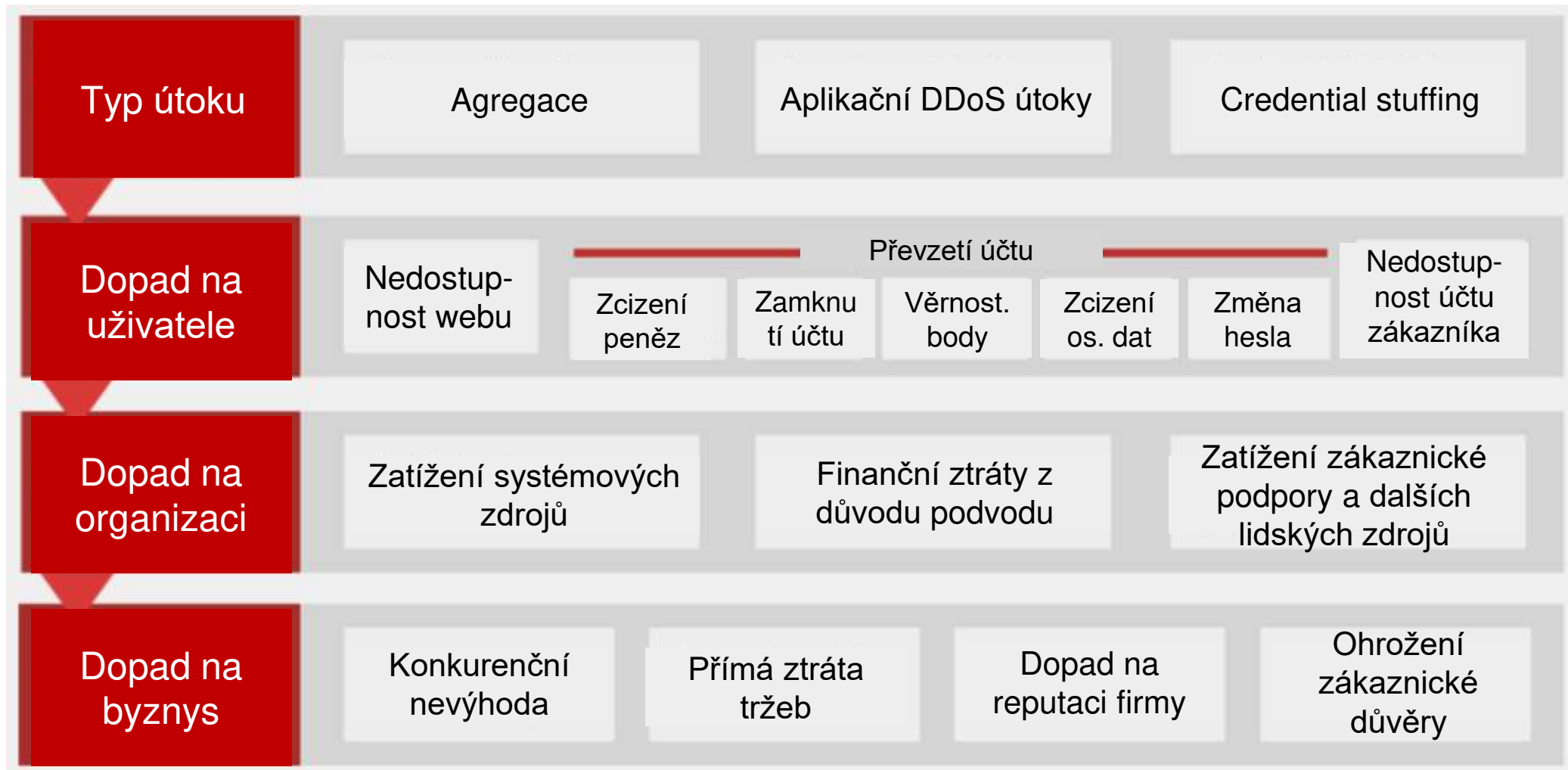
POSTS TO /LOGIN EVERY THREE HOURS

● HUMAN

● DETECTED & FLAGGED

● DETECTED & BLOCKED





Platforma Shape Security

Shape Defense

Identify and mitigate unwanted traffic



Bots



Human Clickfarm

Shape AI Fraud Engine - SAFE

Differentiate good customers from bad customers



Fraudsters and Criminals

Recognize

Create a friction free user experience and increase revenue



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)



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

