Igor Hák
igor.hak@eset.cz

Moderní hrozby

Co se nezměnilo?

Co se nezměnilo?

- Uživatel stále nejslabším článkem
- Soustředění útočníků na
  - platformy s největším podílem
  - „bohaté“ sektory

Trocha statistiky

Pohled na data a statistiku

welivesecurity™

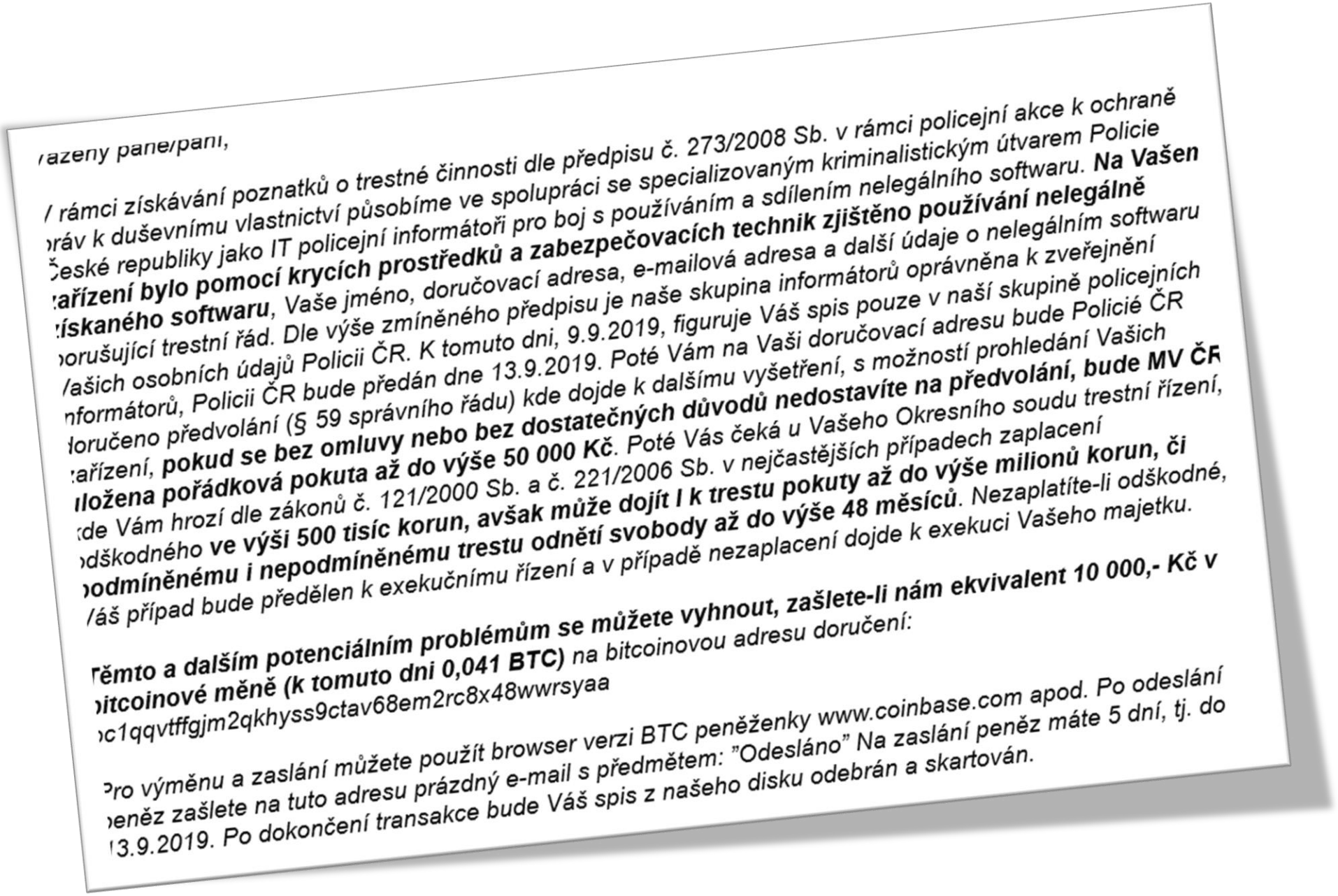
STATISTICS & TRENDS

Category	T1 2022/ T2 2022	Key points in T2 2022
Overall threat detections	-9.1% ↓	Decrease in detections in almost all monitored categories
Infostealers	-14.3% ↓	JS/Spy.Banker (aka Magecart) remains top banking malware
Ransomware	-24.1% ↓	Politically motivated ransomware on the decline
Downloaders	-31.0% ↓	Emotet continues activity, adapts distribution vectors
Cryptocurrency threats	-16.0% ↓	Cryptostealers see first period of growth, at almost 50%
Web threats	-6.0% ↓	Surge in shipping-themed phishing lures
Email threats	-10.2% ↓	Office files double their share among malicious attachments
Android	+9.5% ↑	Android spyware continues its growth from T1
macOS	-15.1% ↓	Decline in detections most prominent in the Adware category
RDP attacks	-89.4% ↓	RDP attacks fall further, following sharp T1 decline

Sociální inženýrství – „oblbování“ uživatelů

NAZDÁREK

Jsem Albánský počítačový virus
ABDUL.exe.
S ohledem na mizivé možnosti mé
země ti nemůžu nic udělat.
V rámci humanitární pomoci si smaž
ve svém počítači nějaký soubor a
pošli mě dál !



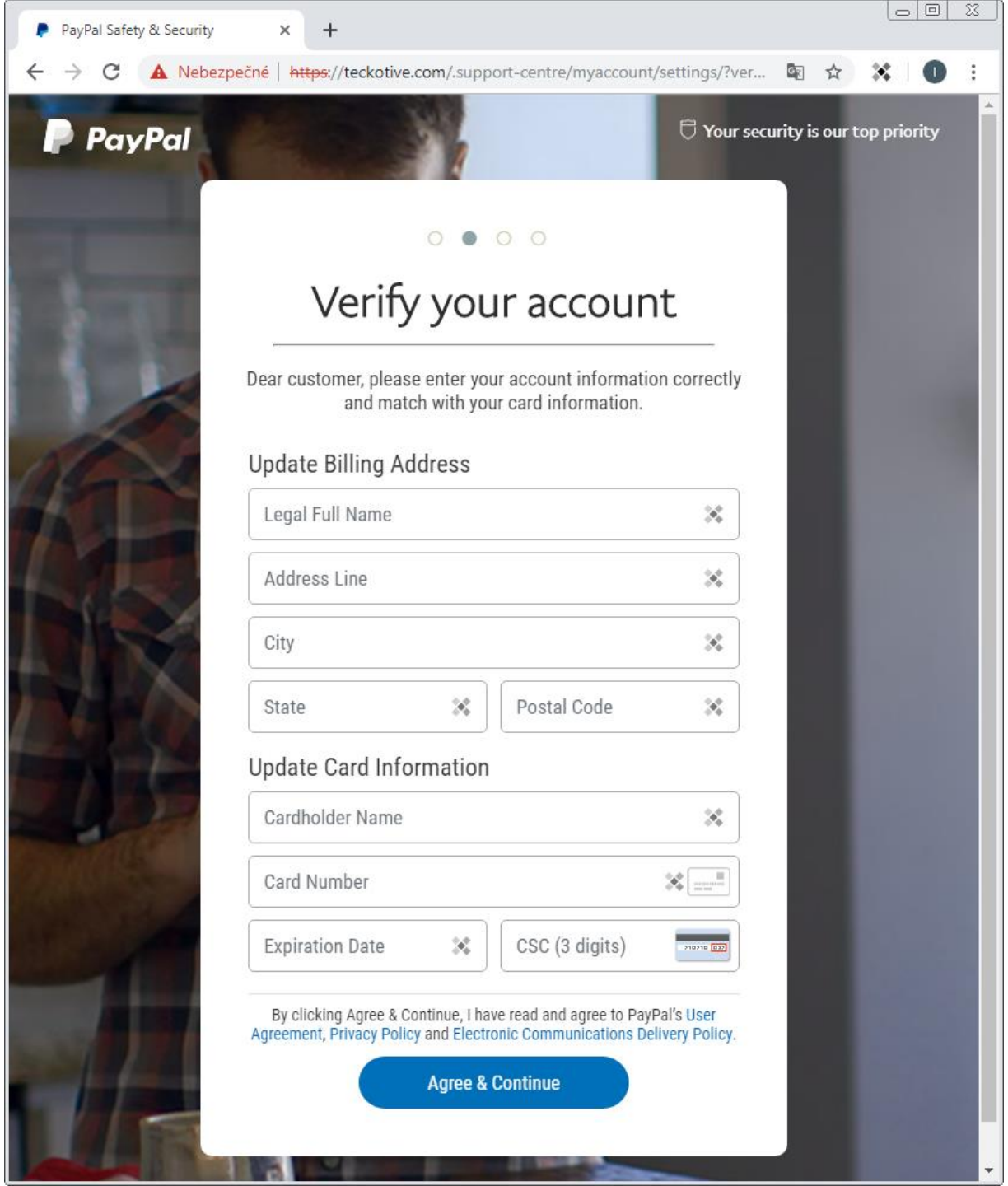
Vážený pane/paní,

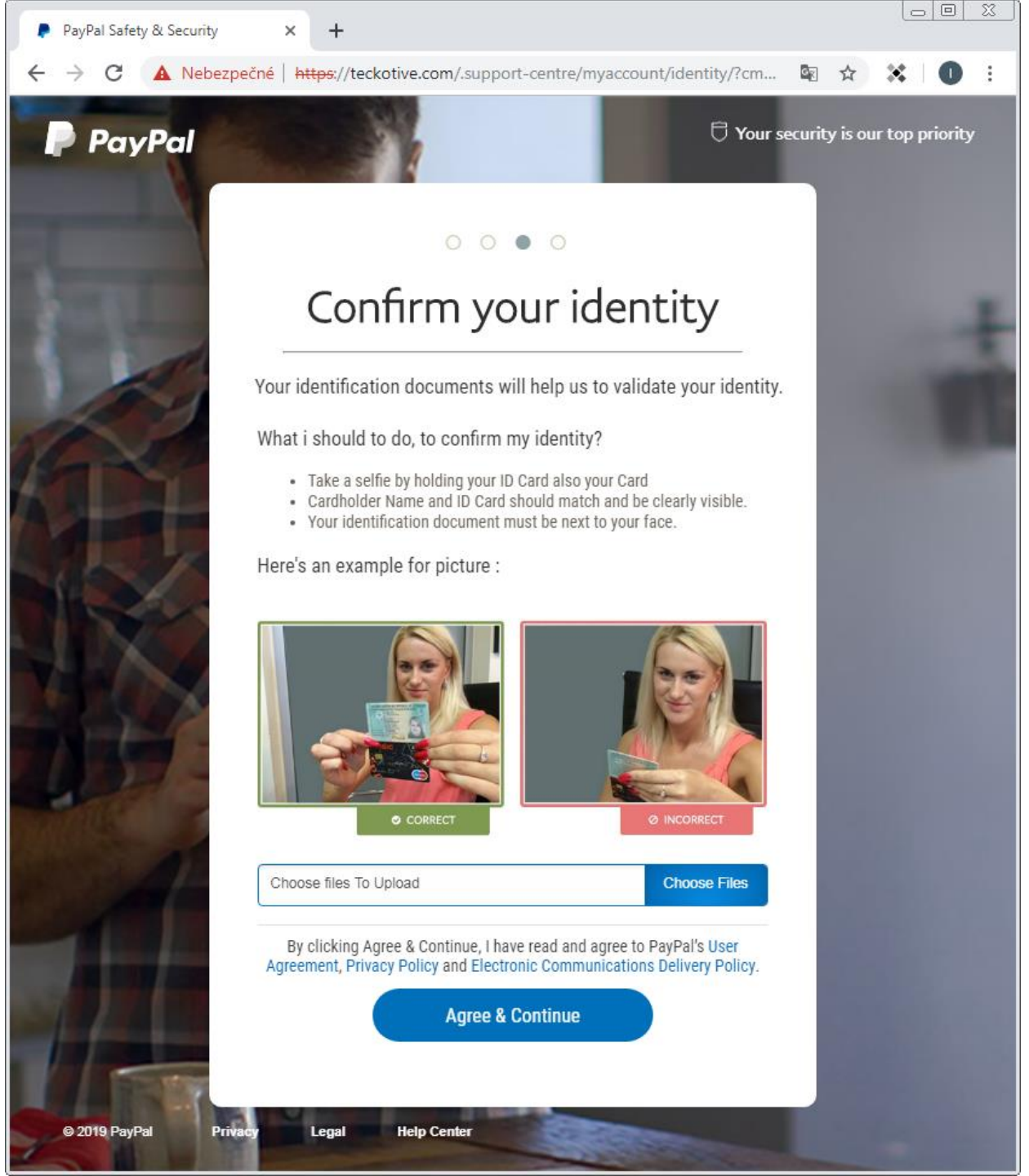
V rámci získávání poznatků o trestné činnosti dle předpisu č. 273/2008 Sb. v rámci policejní akce k ochraně práv k duševnímu vlastnictví působíme ve spolupráci se specializovaným kriminalistickým útvarem Policie České republiky jako IT policejní informátoři pro boj s používáním a sdílením nelegálního softwaru. **Na Vašem zařízení bylo pomocí krycích prostředků a zabezpečovacích technik zjištěno používání nelegálně získaného softwaru**, Vaše jméno, doručovací adresa, e-mailová adresa a další údaje o nelegálním softwaru porušující trestní řád. Dle výše zmíněného předpisu je naše skupina informátorů oprávněna k zveřejnění Vašich osobních údajů Policii ČR. K tomuto dni, 9.9.2019, figuruje Váš spis pouze v naší skupině policejních informátorů, Policii ČR bude předán dne 13.9.2019. Poté Vám na Vaši doručovací adresu bude Policié ČR doručeno předvolání (§ 59 správního řádu) kde dojde k dalšímu vyšetření, s možností prohledání Vašich zařízení, **pokud se bez omluvy nebo bez dostatečných důvodů nedostavíte na předvolání, bude MV ČR uložena pořádková pokuta až do výše 50 000 Kč**. Poté Vás čeká u Vašeho Okresního soudu trestní řízení, kde Vám hrozí dle zákonů č. 121/2000 Sb. a č. 221/2006 Sb. v nejčastějších případech zaplacení odškodného **ve výši 500 tisíc korun, avšak může dojít I k trestu pokuty až do výše milionů korun, či podmíněnému i nepodmíněnému trestu odnětí svobody až do výše 48 měsíců**. Nezaplatíte-li odškodné, Váš případ bude předělen k exekučnímu řízení a v případě nezaplacení dojde k exekuci Vašeho majetku.

Těmto a dalším potenciálním problémům se můžete vyhnout, zašlete-li nám ekvivalent 10 000,- Kč v bitcoinové měně (k tomuto dni 0,041 BTC) na bitcoinovou adresu doručení:

bc1qqvtffgjm2qkhyss9ctav68em2rc8x48wwrsyaa

Pro výměnu a zaslání můžete použít browser verzi BTC peněženky www.coinbase.com apod. Po odeslání peněz zašlete na tuto adresu prázdný e-mail s předmětem: "Odesláno" Na zaslání peněz máte 5 dní, tj. do 13.9.2019. Po dokončení transakce bude Váš spis z našeho disku odebrán a skartován.





Menu upomínka úhrady faktury číslo 074012318

Odpovědět Odpovědět všem Předat dál

upomínka úhrady faktury číslo 074012318

Od Kinga Lipowska
komu petr

ne 2.12.2018 23:26

Vydana_faktura_074012318.rar (67 kB)

Dobrý den,

při kontrole našich dokladů jsme zjistili, že jste dosud neuhradili naši pohledávku číslo 074012318 za Kroměříž -> Červený Kostelec na částku 3337,00 Kč, splatnou dne 29.10.2018.

Předpokládáme, že se jedná o pouhé opomenutí a že dlužnou pohledávku neprodleně uhradíte.

Pokud jste uvedenou pohledávku již uhradili, sdělte nám prosím informace o způsobu a termínu platby.

S pozdravem,

Kinga Lipowska

DS

Domain Service info@shaxiakey.top

17. 2. 2020, 6:01

Komu: igi@viry.cz

epj.cz expiration

Important notice

Notice#: 719677
Date: 02/17/2020

Domain Expiration

Domain: epj.cz

Expiration date: 02/25/2020

To: Igor Hak,
Okružní 2316
Dvůr Králové nad Labem
, 544 01
CZECH REPUBLIC

Domain Name:	Registration Period:	Amount:	Term:
epj.cz	03/10/2020 to 03/10/2021	$86.00	1 Year

Secure Online Payment

Domain Name: epj.cz
Attn: Igor Hak

20:21 43%

+420 721 639 080
online

ZABLOKOVAT | PŘIDAT

Včera

Zprávy a hovory jsou zabezpečeny koncovým šifrováním. Nikdo, kdo není přímým účastníkem této konverzace, ji nemůže sledovat ani poslouchat. Dokonce ani WhatsApp. Další informace zobrazíte klepnutím.

BabyDan detska zábrana New Flex XXL 90-350 cm - Trutnov | ...
Inzerát č. 148505204: BabyDan detsk...
deti.bazos.cz

Dobrý den, viděl jsem váš inzerát a zajímalo by mě, zda prodáváte?
https://deti.bazos.cz/inzerat/148505204/babydan-detska-zabrana-new-flex-xxl-90-350-cmn.php
22:18

zdravim, ano 22:33

Přesně to, co potřebuji! Vyhovuje mi to, jsem připraven si to od vás koupit. Řekněte mi, ve kterém městě žijete?
22:42

trutnov 22:54

Problém! Žiji v Dačicíce. Nebude vám vadit, když k vám pošlu kurýra zasilkovnou nebo dpd? Veškeré náklady na kurýra za vás uhradím! Jsem připraven zaplatit i bankovním převodem.
23:13

ok 23:36

Dnes

souhlasim, nevadi 0:12

dobry den, jak provedeme to doruceni?
9:46

Dobře, připravím informační formulář a pošlu bance žádost o schválení transakce. Až bude vše dokončeno, odešlu vám transakci a počkám na vás v okně transakce, abychom mohli převést peníze na váš účet.
19:50

Vše je připraveno a schváleno! Pojďte dál, budu na vás čekat u okénka s nabídkami.
19:51

BabyDan detska zábrana New Flex XXL 90-350 cm
Find all ads for BabyDan detska zábrana New Fl...
dpd-cz.seznam-spay.com

https://dpd-cz.seznam-spay.com/cash98549348
19:51

Zpráva

20:22 42%

pd-cz.seznam-spay.com 35

Získání finančních prostředků

VISA

Transakce prostřednictvím bankovních karet VISA nebo MasterCard. Bezpečnost manipulace s plastovými kartami zaručuje Equa bank.

Číslo karty

0000 0000 0000 0000

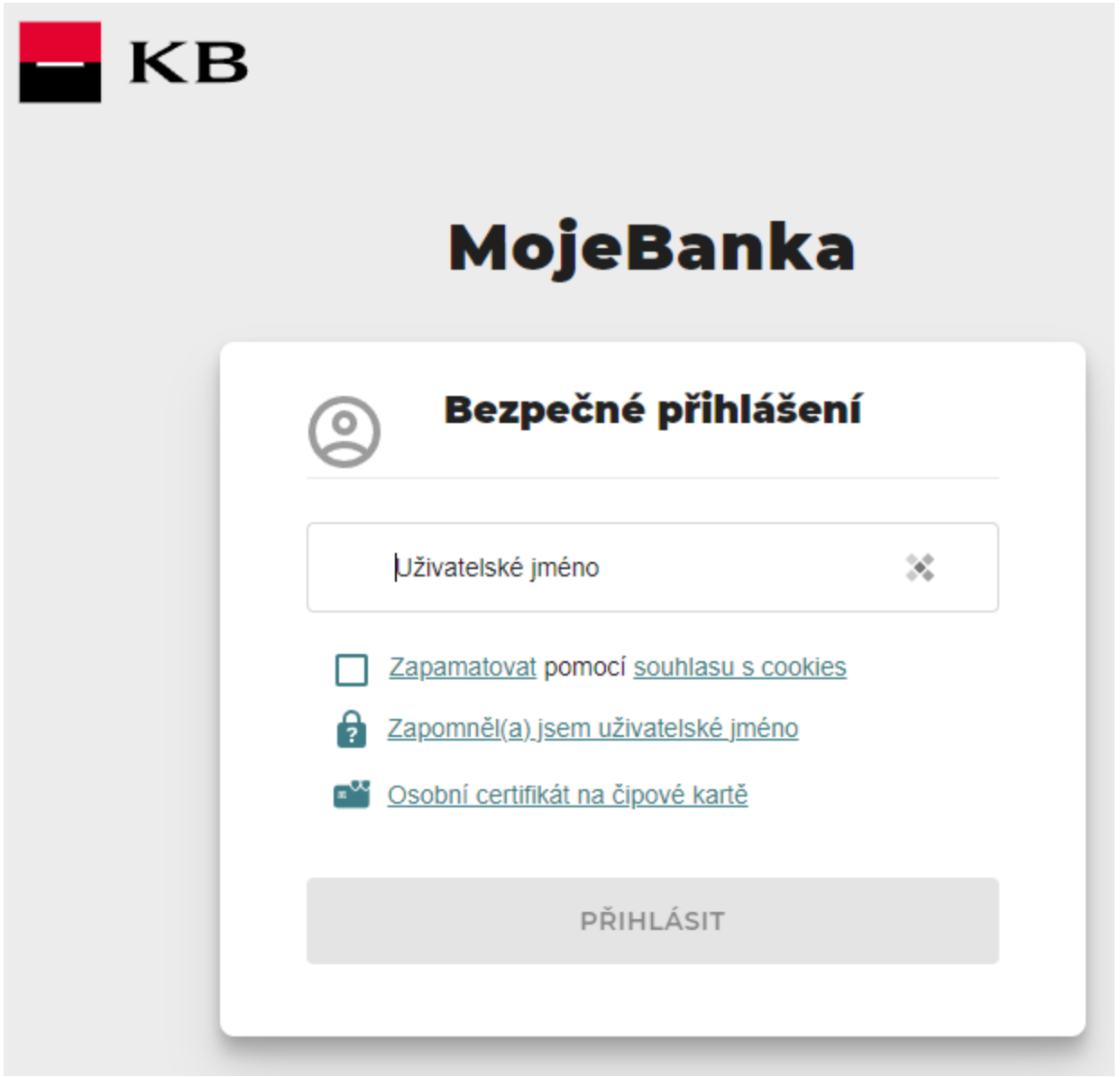
Doba platnosti **CVC kód**

04 | 20 | •••

K získání: 3400 Kč

Vaše data jsou bezpečně chráněna.

ZPĚT POKRAČOVAT



TABORSKY
deník.cz

ZPRÁVY SPORT PODNIKÁNÍ NÁZORY MAGAZÍN PODCASTY MIMINKA O DENÍK

TÁBORSKO Z OKOLÍ ENERGIE KRIMI KULTURA TIPY ČEŠI V ČÍSLECH ČTENÁŘ REPORTÉR

DŮCHODOVÁ KALKULAČKA Spočítejte si, o kolik se vám od ledna 2023 zvýší penze

Další oběť IT podvodu je z Tábora. Chtěl prodat přilbu, přišel o tři sta tisíc

21.10.2022

Zuzana Gabajová
Editorka
Napište mi

Řady obětí internetových podvodů rozšířil muž z Tábora, který zadal na falešnou stránku přihlašovací údaje ke svému bankovnímu účtu a přišel o statisíce korun.

SPECIÁLNÍ ZPRÁVA: Nejnovější investice Dominika Stroukala uvedla odborníky v úžas a velké banky se začínají děsit

Češi si už z pohodlí svého domova stačili vydělat miliony korun používáním této „skuliny k bohatství" – jde ale o legitimní věc?

lidovky
Zpravodajský server Lidových novin

Independent.ie

AS SEEN ON BBC WORLD NEWS

iDNES.cz

díky které bohatnou už stovky Stroukalů

VÝSLEDKY ČTENÁŘŮ

ZISK: 141 576 Kč

„Používám CryptoBoom jen něco přes 2 týdny a z mého vkladu v hodnotě 6 500,- je dnes 148 076 Kč. To je daleko víc, než si vydělám v práci."

Michal Najman
Hradec Králové

ZISK: 234 600 Kč

„Dosáhl jsem na zisk necelých 235 000 Kč, a to už po jednom měsíci používání CryptoBoom . Můžu to používat na laptopu, takže si v klidu cestuji a vydělávám peníze!"

Jan Filipi

SPECIALNI ZPRAVA: Nejnovější investice Jaromíra Soukupa uvedla odborníky v úžas a velké banky se začínají děsit

Češi si už z pohodlí svého domova stačili vydělat miliony korun používáním této „skuliny k bohatství" – jde ale o legitimní věc?

AS SEEN ON

lidovky.cz · Independent.ie · BBC WORLD NEWS · A · iDNES.cz

...řišel s novou tajnou investicí, díky které bohatnou už stovky Soukupů

VÝSLEDKY

ZISK: 141 576 Kč

„Používám CryptoBoom jen něco přes 2 týdny a z mého vkladu v hodnotě 6 500,- je dnes 148 0[illegible]6 Kč. To je daleko víc, než si vydělám v práci."

Michal Najman
Hradec Králové

ZISK: 234 600 Kč

„Dosáhl jsem na zisk necelých 235 000 Kč, a to už po jednom měsíci používání CryptoBoom . Můžu to používat na laptopu, takže si v klidu cestuji a vydělávám peníze!"

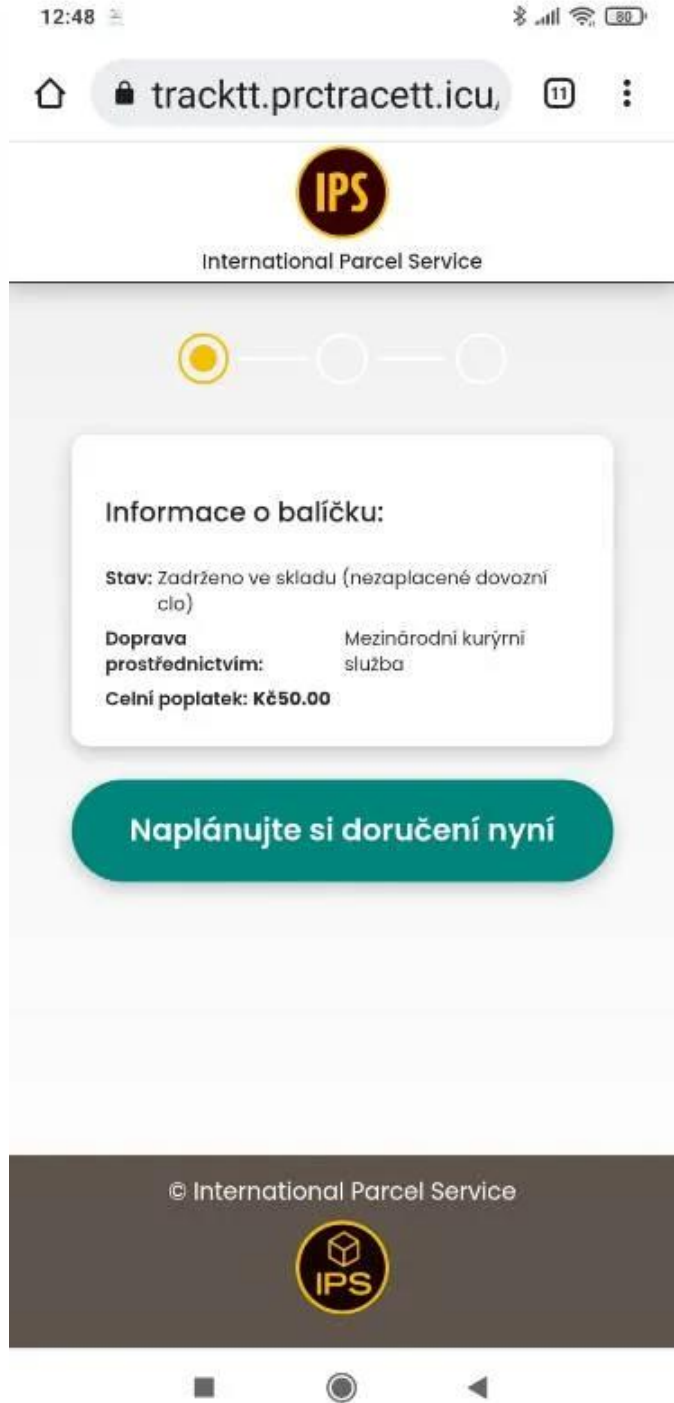
Jan Filipi

FINANČNÍ SPRÁVA

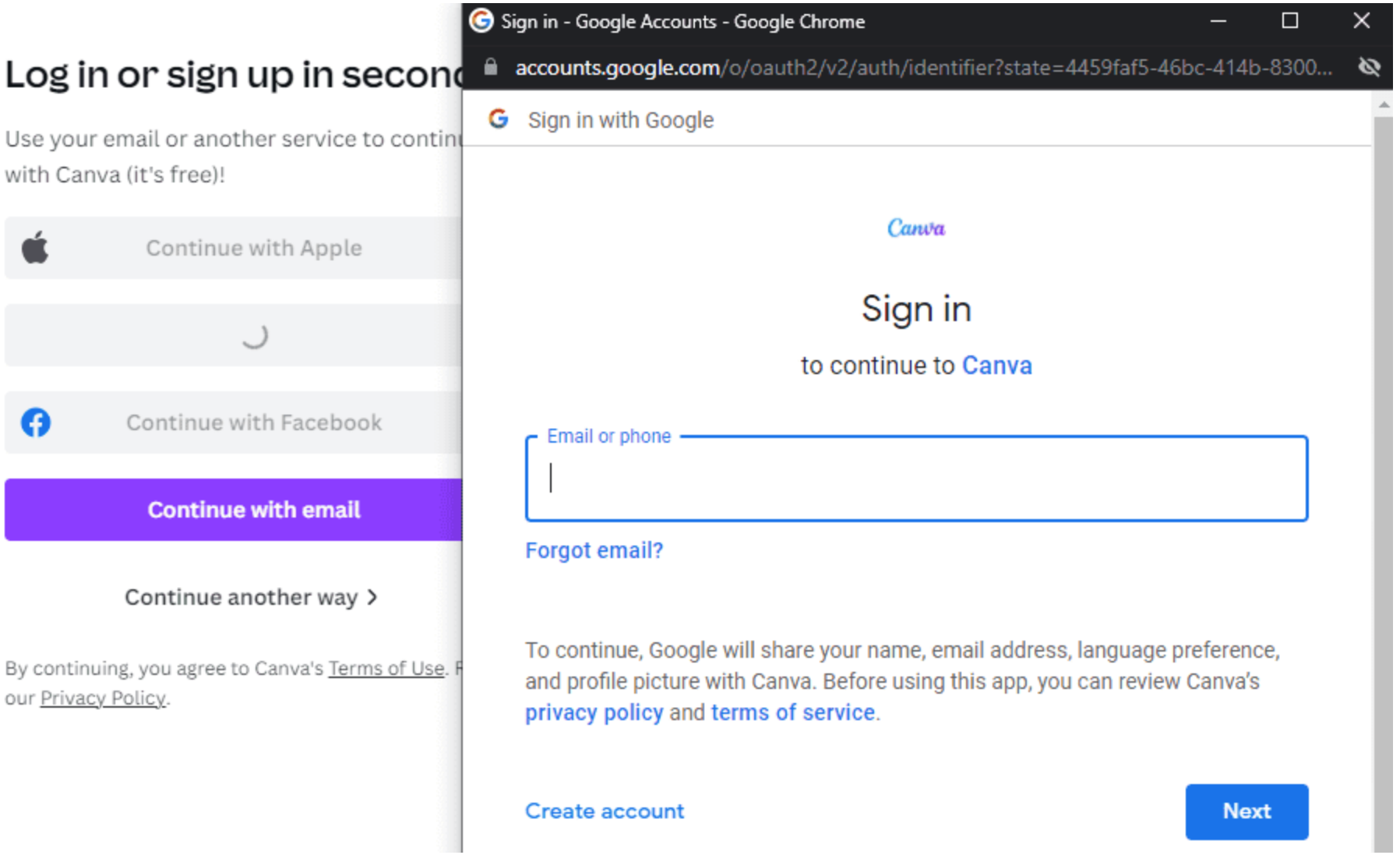
Máte nárok na vrácení částky 136,99 EUR.
Zašlete prosím následující formulář, abychom ho mohli zpracovat vrátit se co nejdříve.

klikněte zde

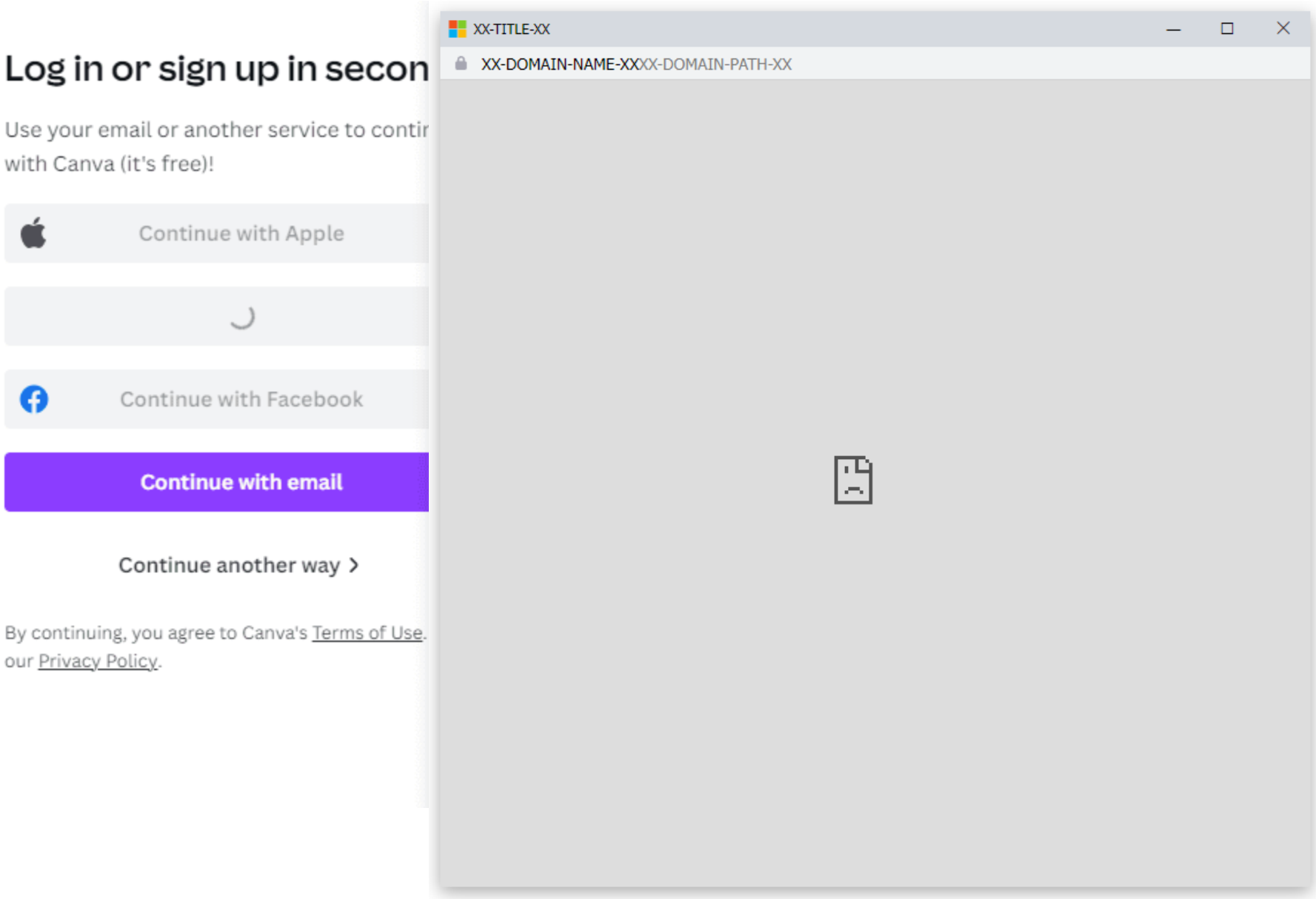
Po přijetí formuláře vám bude naúčtována refundace ekvivalent našich služeb.
Odesílání nebo zaznamenávání neplatného souboru po určitém limitu může oddálit vrácení platby
Brzy dostanete formulář na vrácení platby

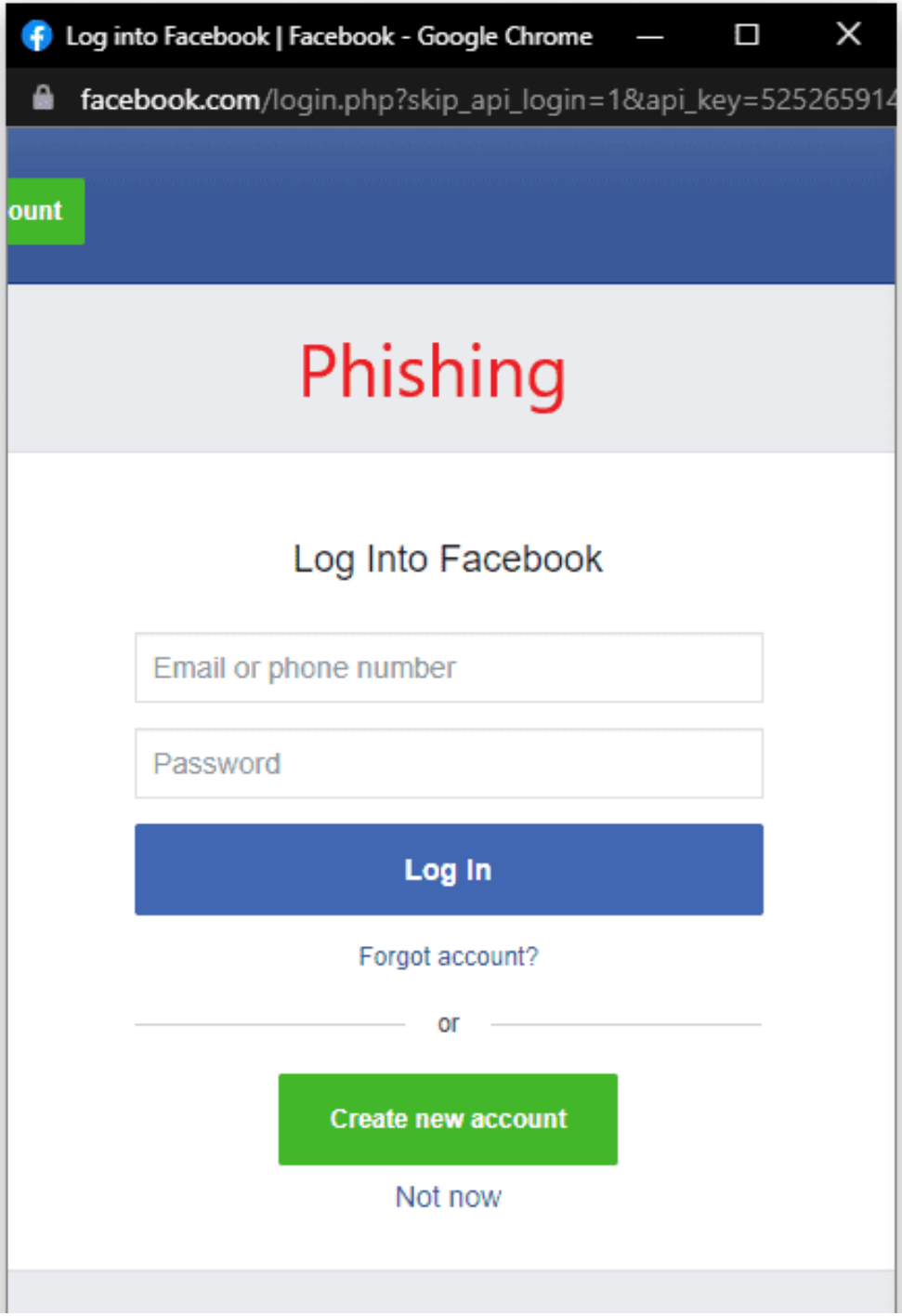


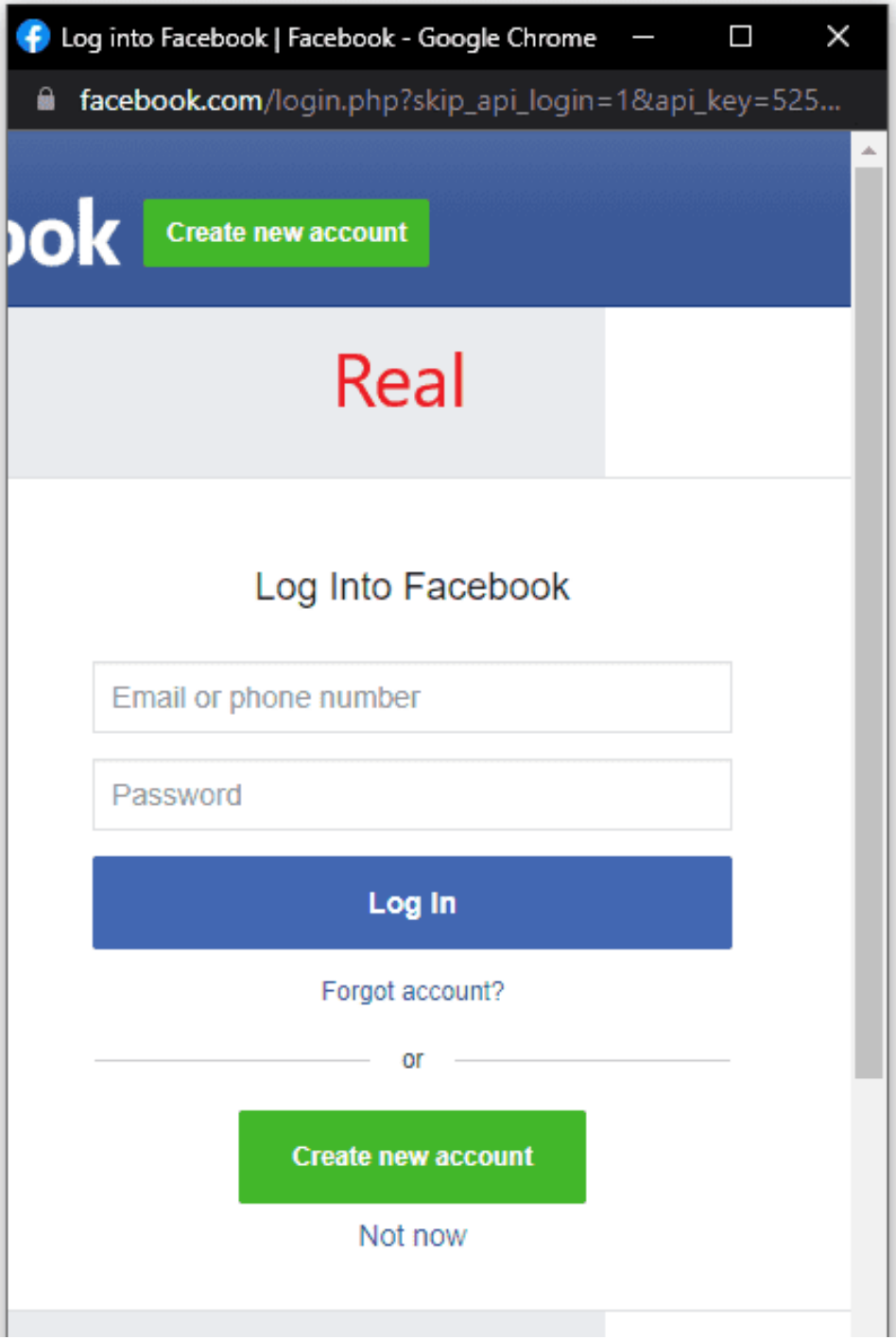
Browser in the Browser



Browser in the Browser

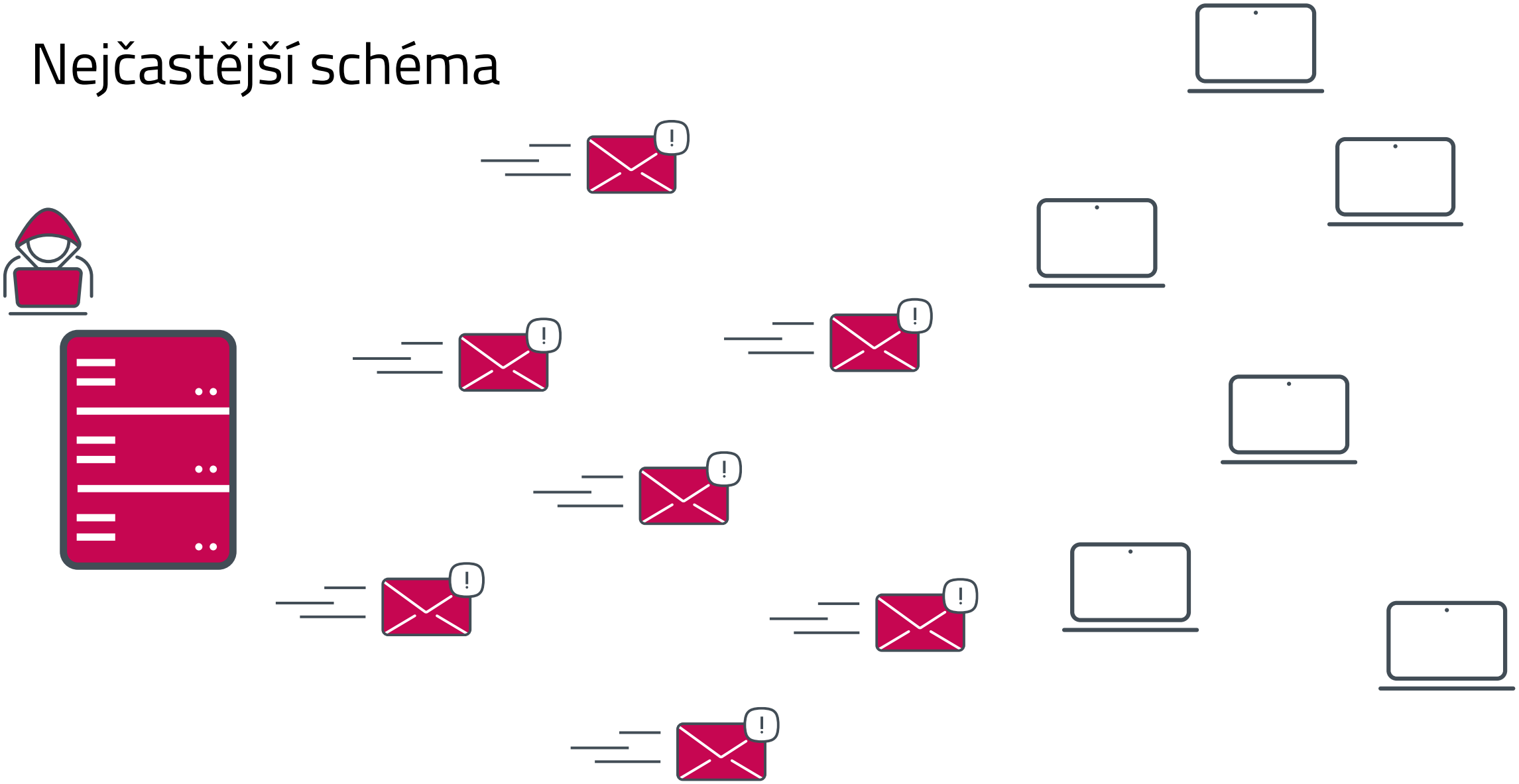






Jak vypadá moderní malware?

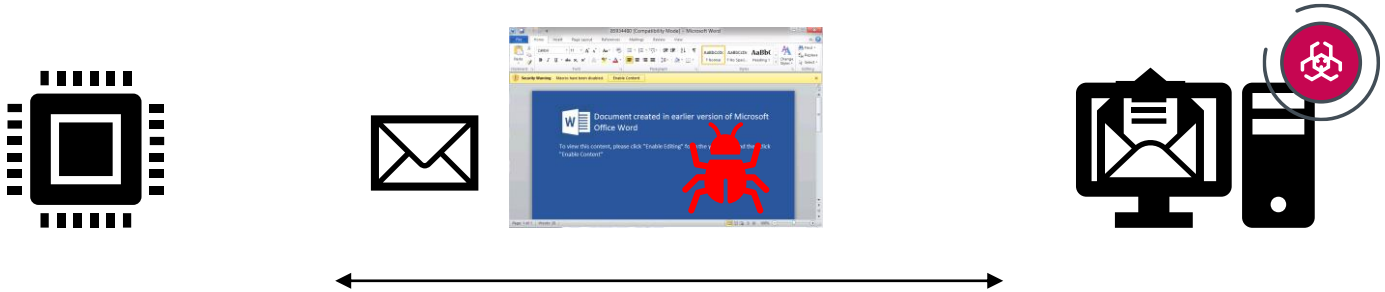
Nejčastější schéma



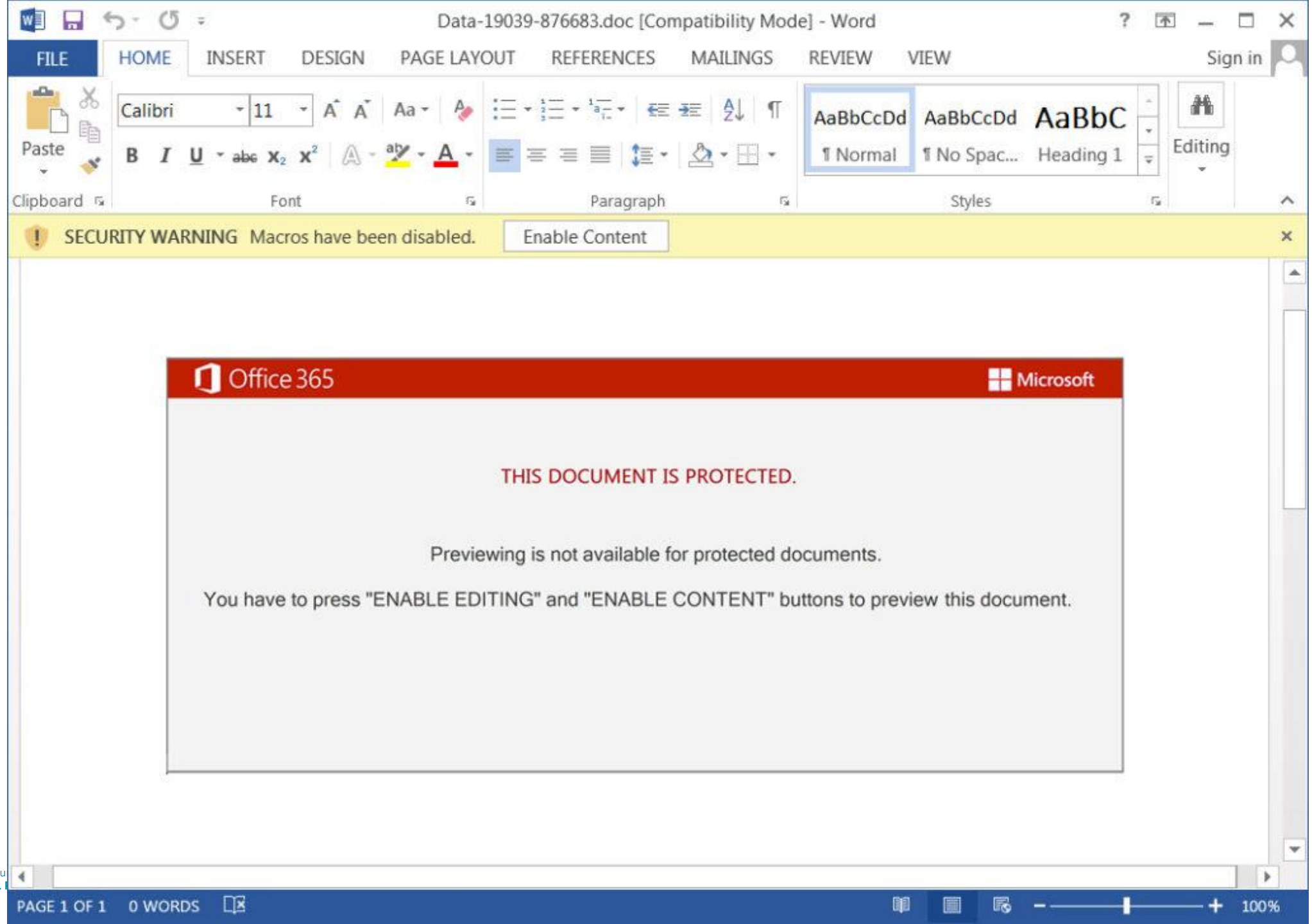
INFEKCE (průnik)

(DOWNLOADER)

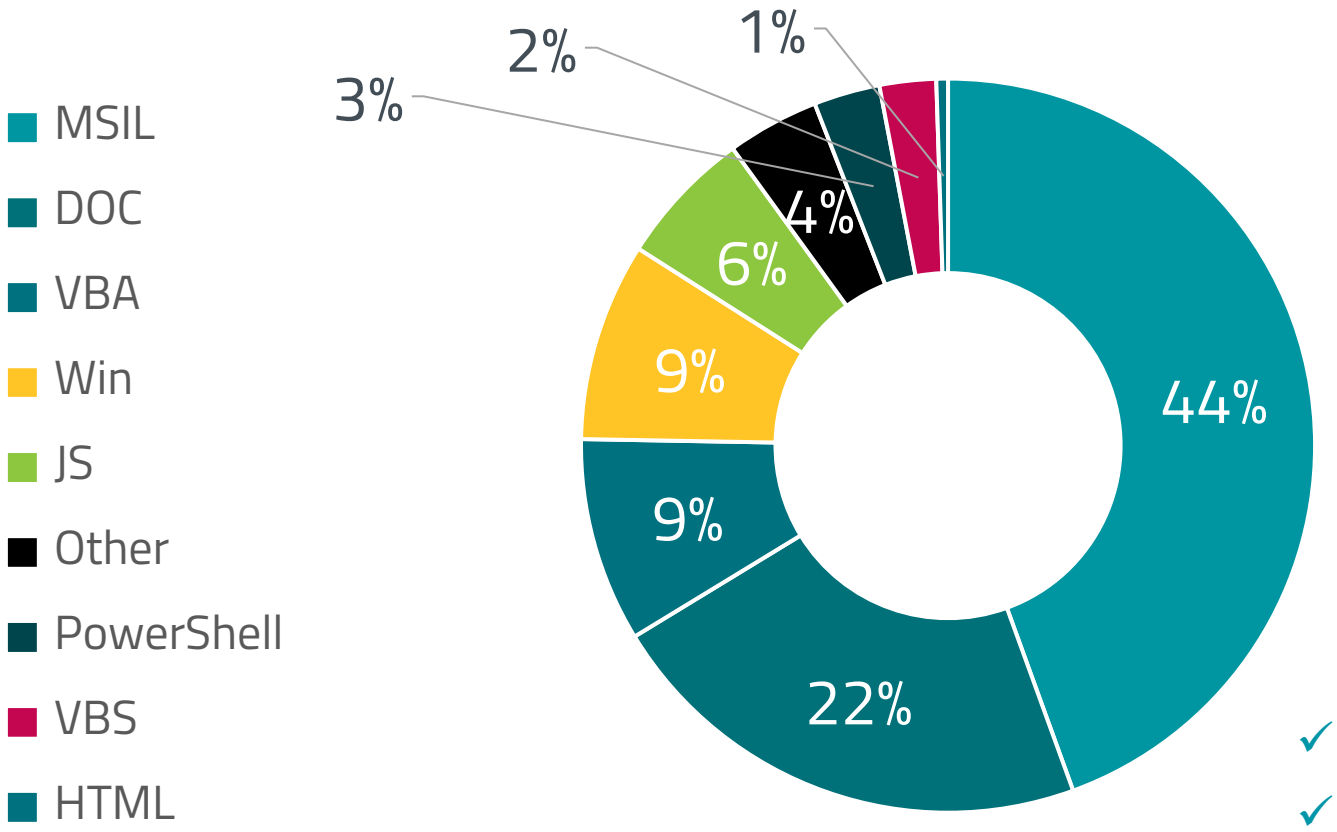
Makro v doc/xls, příloha faktura,Emotet x TrickBot



(RANSOMWARE)


Data-19039-876683.doc [Compatibility Mode] - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Sign in
Paste
Calibri
11
Clipboard
Font
Paragraph
Styles
Editing
AaBbCcDd
¶ Normal
AaBbCcDd
¶ No Spac...
AaBbC
Heading 1
SECURITY WARNING Macros have been disabled.
Enable Content
Office 365
Microsoft
THIS DOCUMENT IS PROTECTED.
Previewing is not available for protected documents.
You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.
PAGE 1 OF 1
0 WORDS
100%

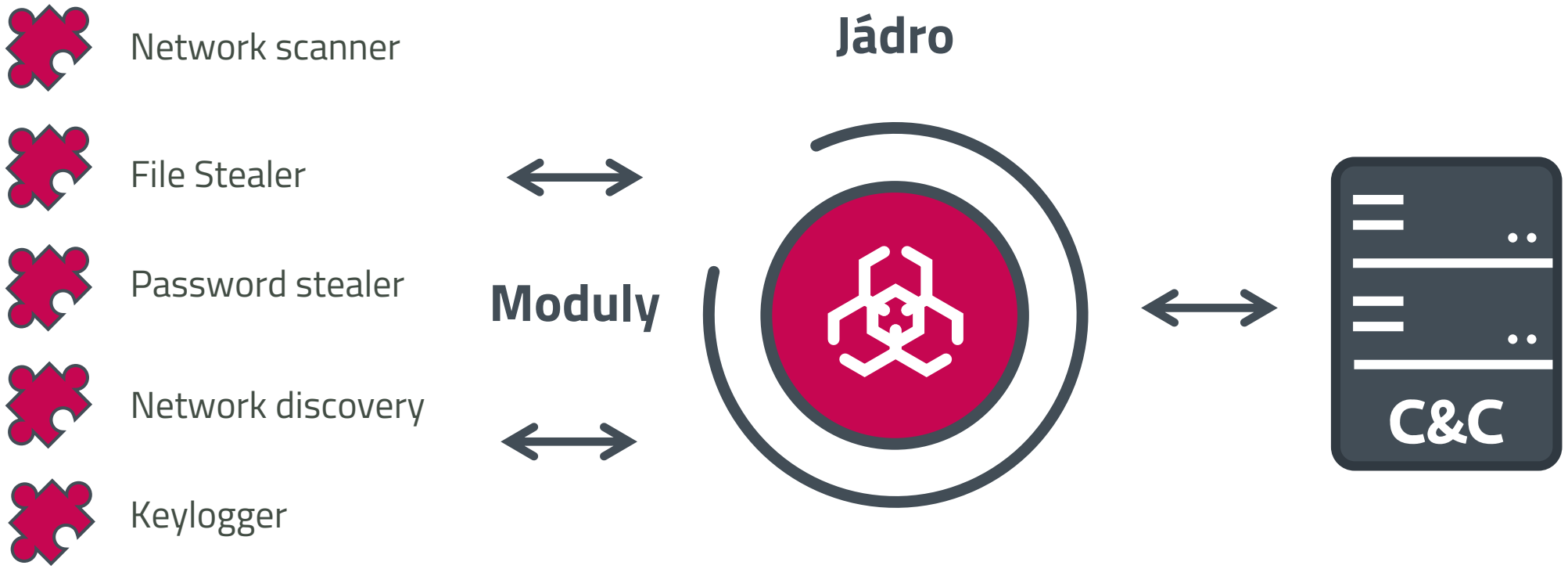
Downloadery - typy souborů v přílohách 2022 ČR



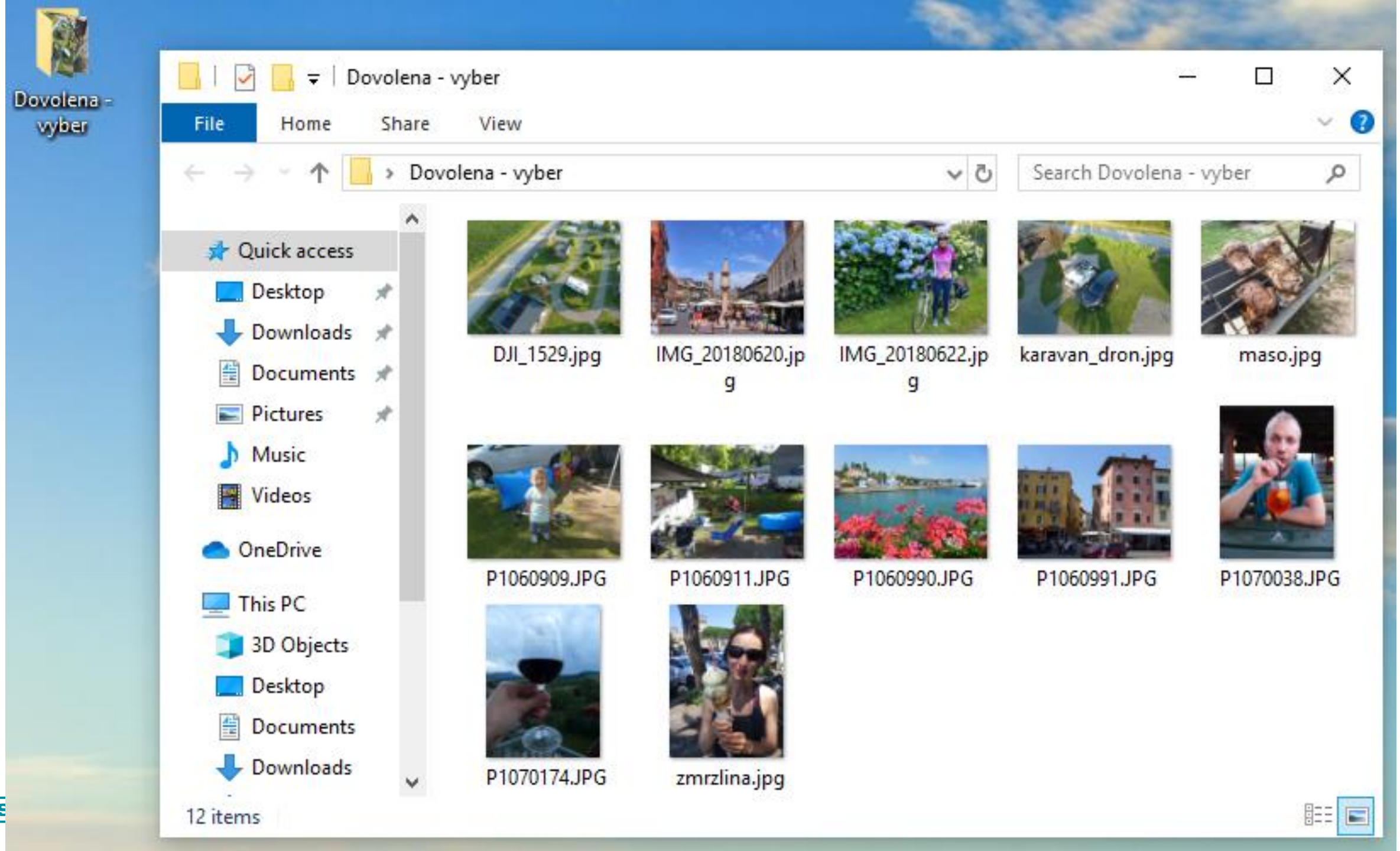
COVID - 19 CSAS DHL Adobe LinkedIn O2 FedEx

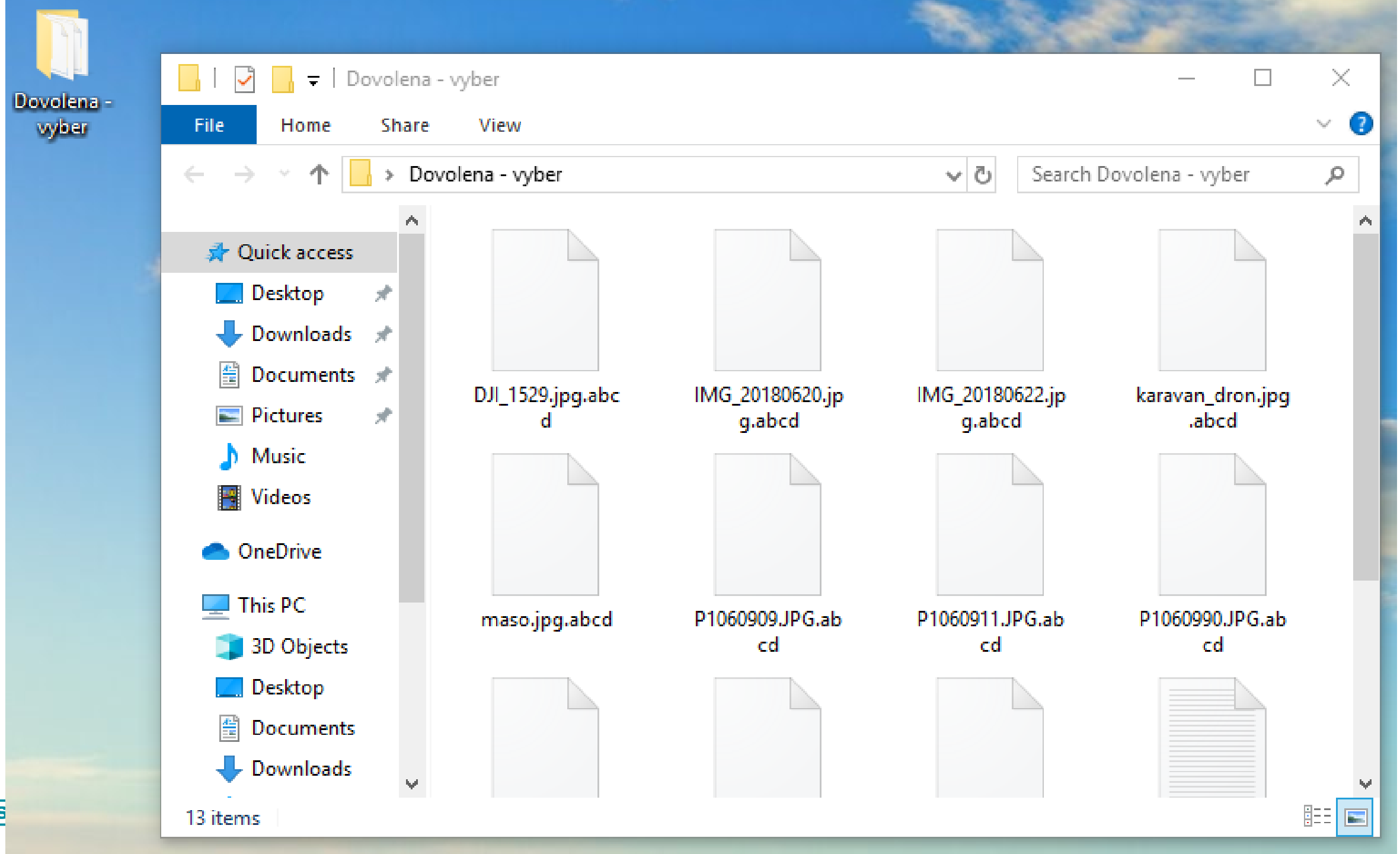
- ✓ Spolu s web stránkami stále nejčastější typ hrozby.
- ✓ Pokles detekcí v květnu a červnu 2022.
- ✓ Zneužívání značek firem (DHL, O2, banky, pošta)
- ✓ Více než polovina příloh spustitelný EXE soubor.

Architektura moderního malware



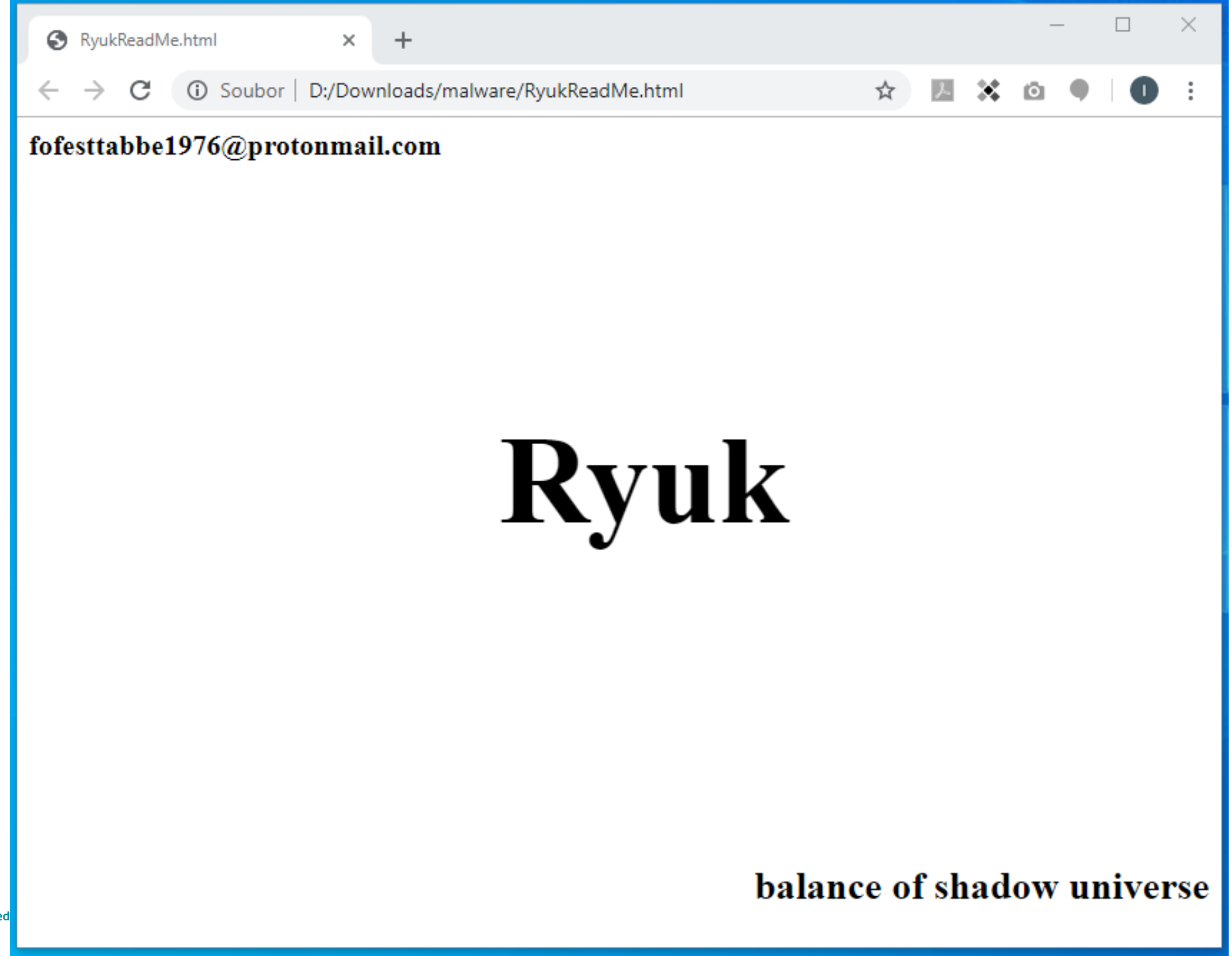
?

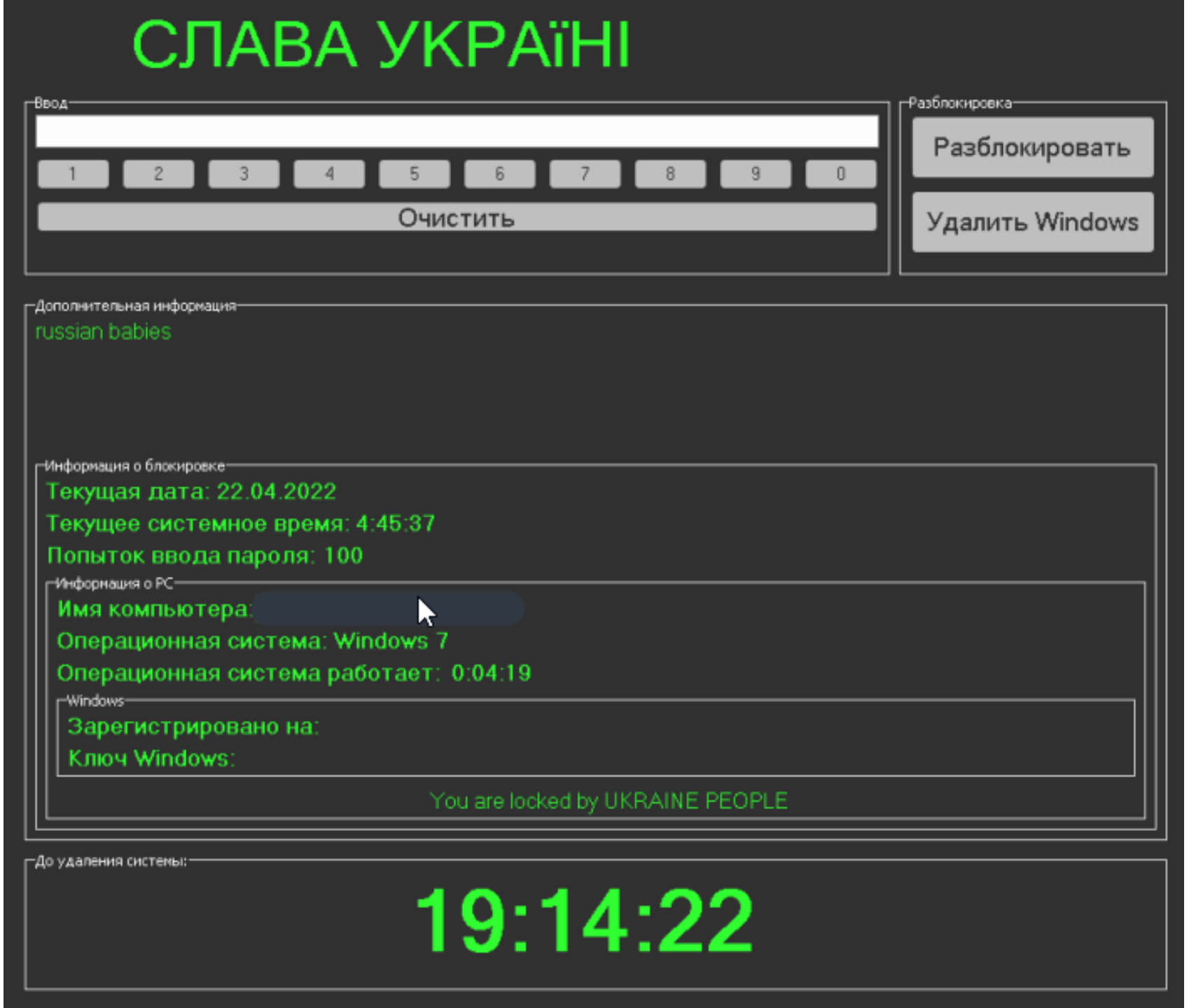

Dovolena - vyber
Dovolena - vyber
File
Home
Share
View
Dovolena - vyber
Search Dovolena - vyber
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
DJI_1529.jpg
IMG_20180620.jpg
IMG_20180622.jpg
karavan_dron.jpg
maso.jpg
P1060909.JPG
P1060911.JPG
P1060990.JPG
P1060991.JPG
P1070038.JPG
P1070174.JPG
zmrzlina.jpg
12 items


Dovolena - vyber
Dovolena - vyber
File
Home
Share
View
Dovolena - vyber
Search Dovolena - vyber
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
DJI_1529.jpg.abcd
IMG_20180620.jpg.abcd
IMG_20180622.jpg.abcd
karavan_dron.jpg.abcd
maso.jpg.abcd
P1060909.JPG.abcd
P1060911.JPG.abcd
P1060990.JPG.abcd
13 items

Ransomware

rEVIL gang





NO REST FOR THE WICKED —

Man gets ransomware porn pop-up, goes to cops, gets arrested on child porn charges

21-year-old walked into police station with computer in hand, cops searched it.

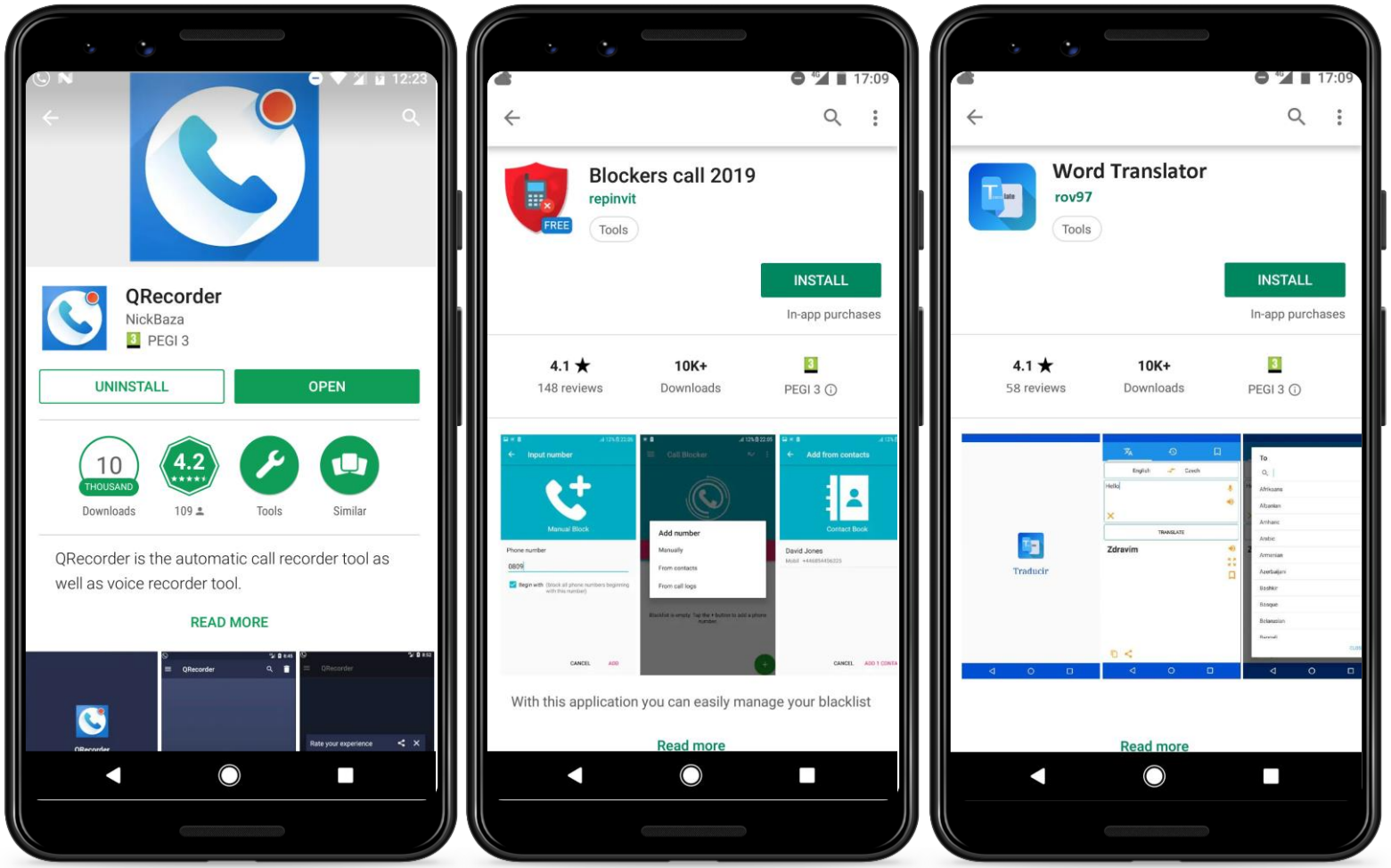
CYRUS FARIVAR - 7/27/2013, 12:50 AM

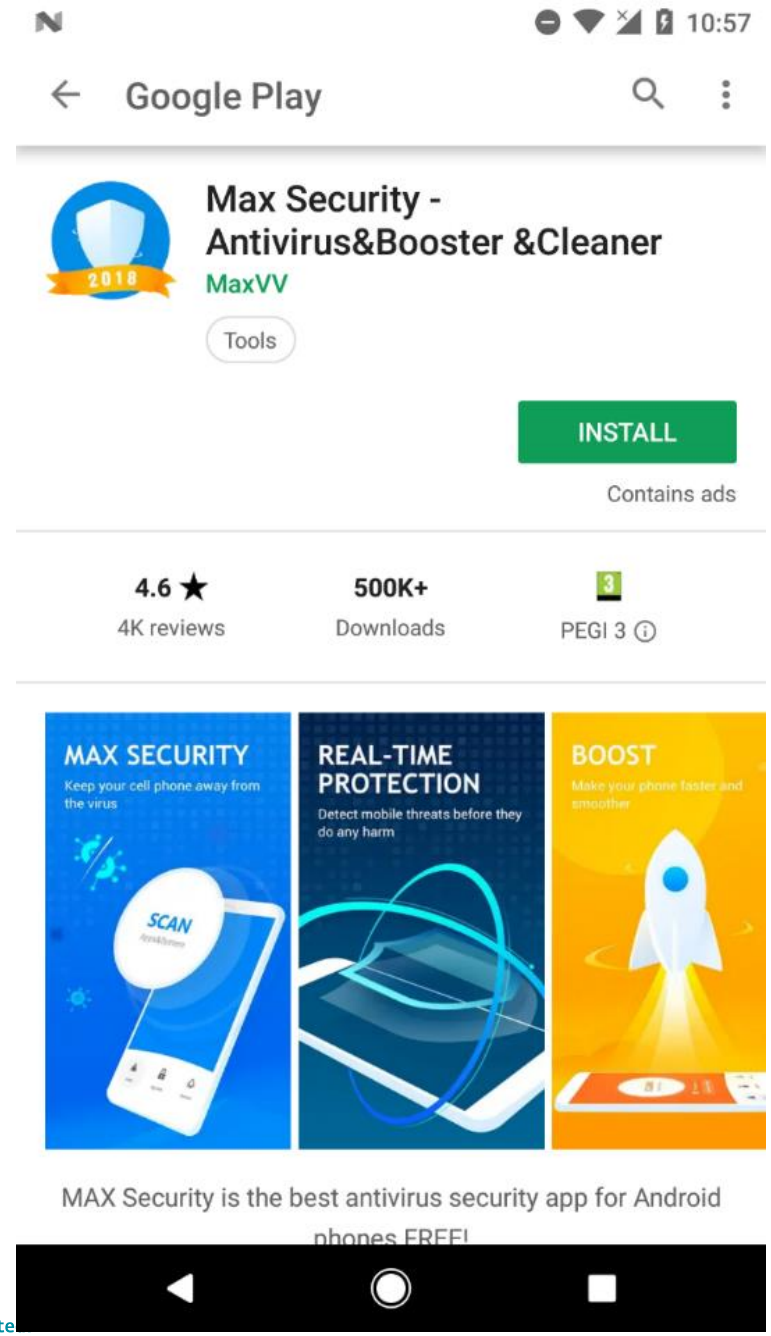
A man from just outside of Washington, DC turned himself in to local police—with his computer in tow—after receiving a pop-up message from what he believed was an "FBI Warning" telling him to click to pay a fine online, or face an investigation.

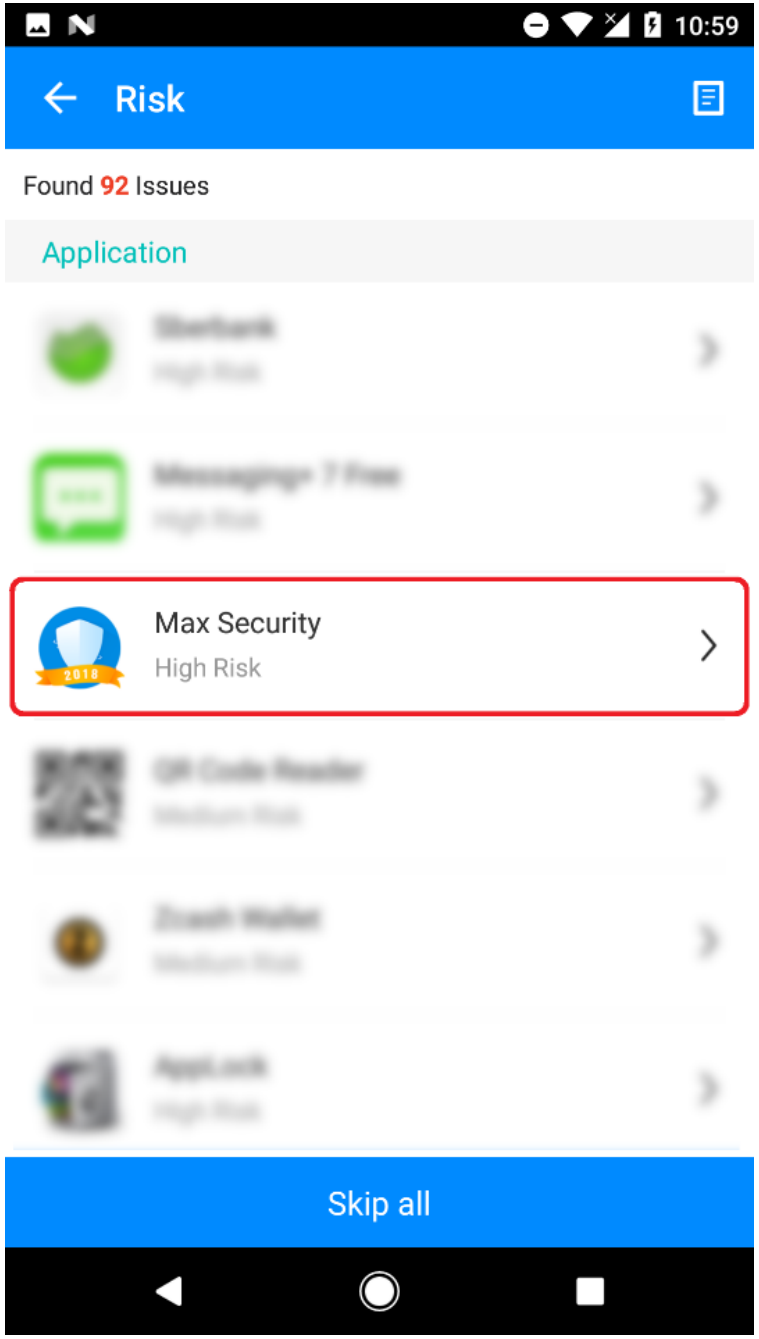
While specific details on the case are scant as of yet, it appears that the suspect here fell victim to a type of ransomware that has been proliferating for years now—raking in millions for the scammers behind it.

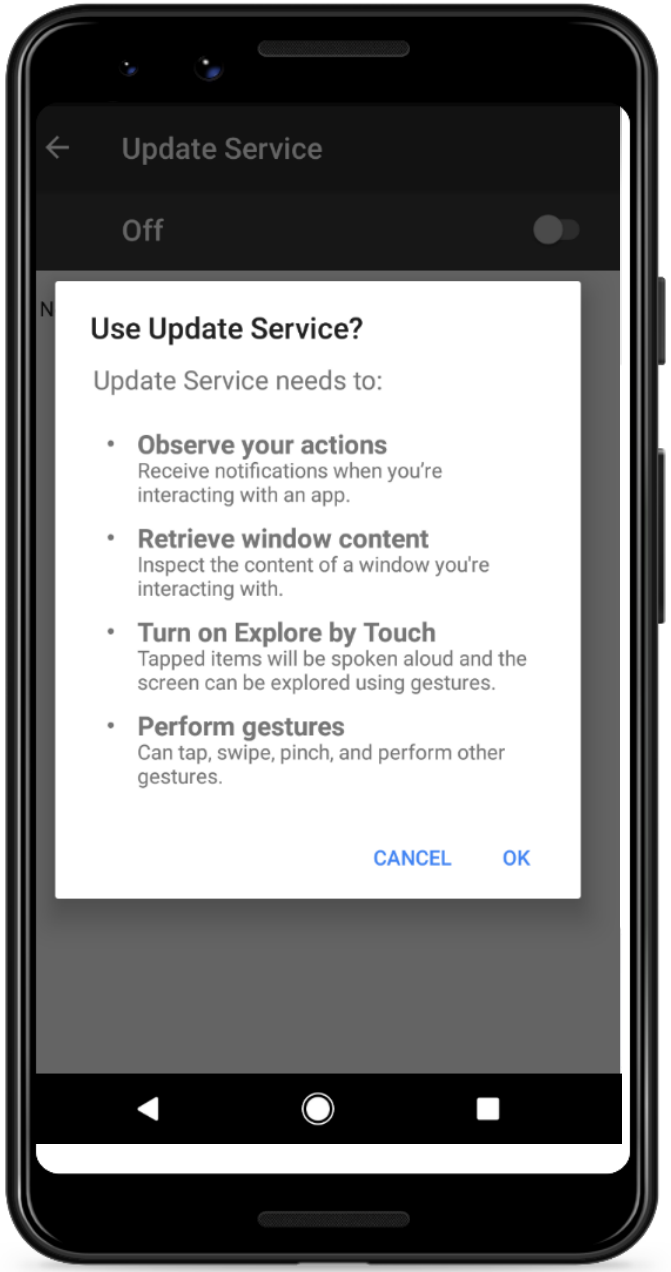
Police said Jay Matthew Riley, 21, of Woodbridge, Virginia, walked into Prince William's Garfield District Station on July 1, 2013 to "inquire if he had any warrants on file for child pornography."

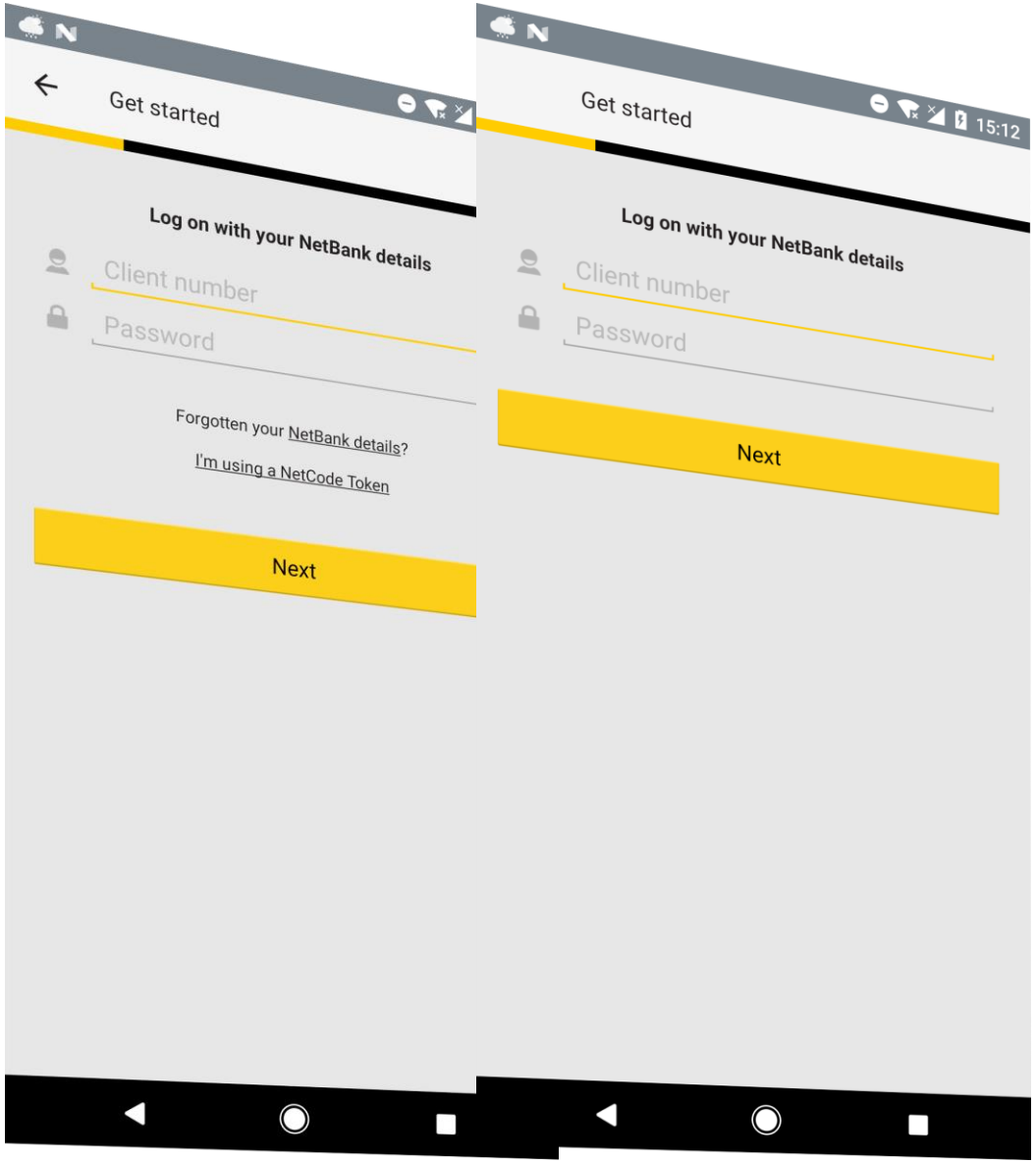
Mobilní zařízení

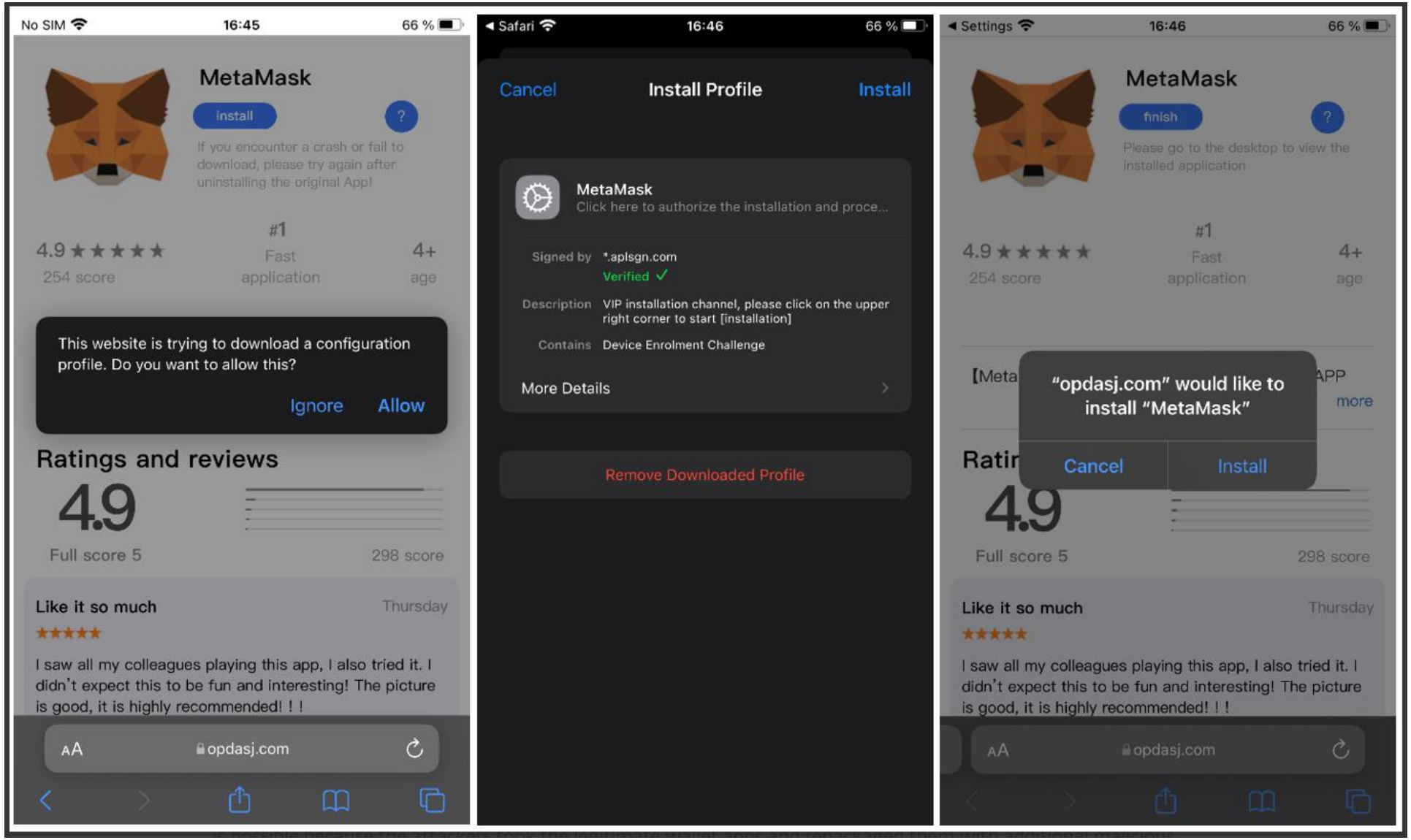




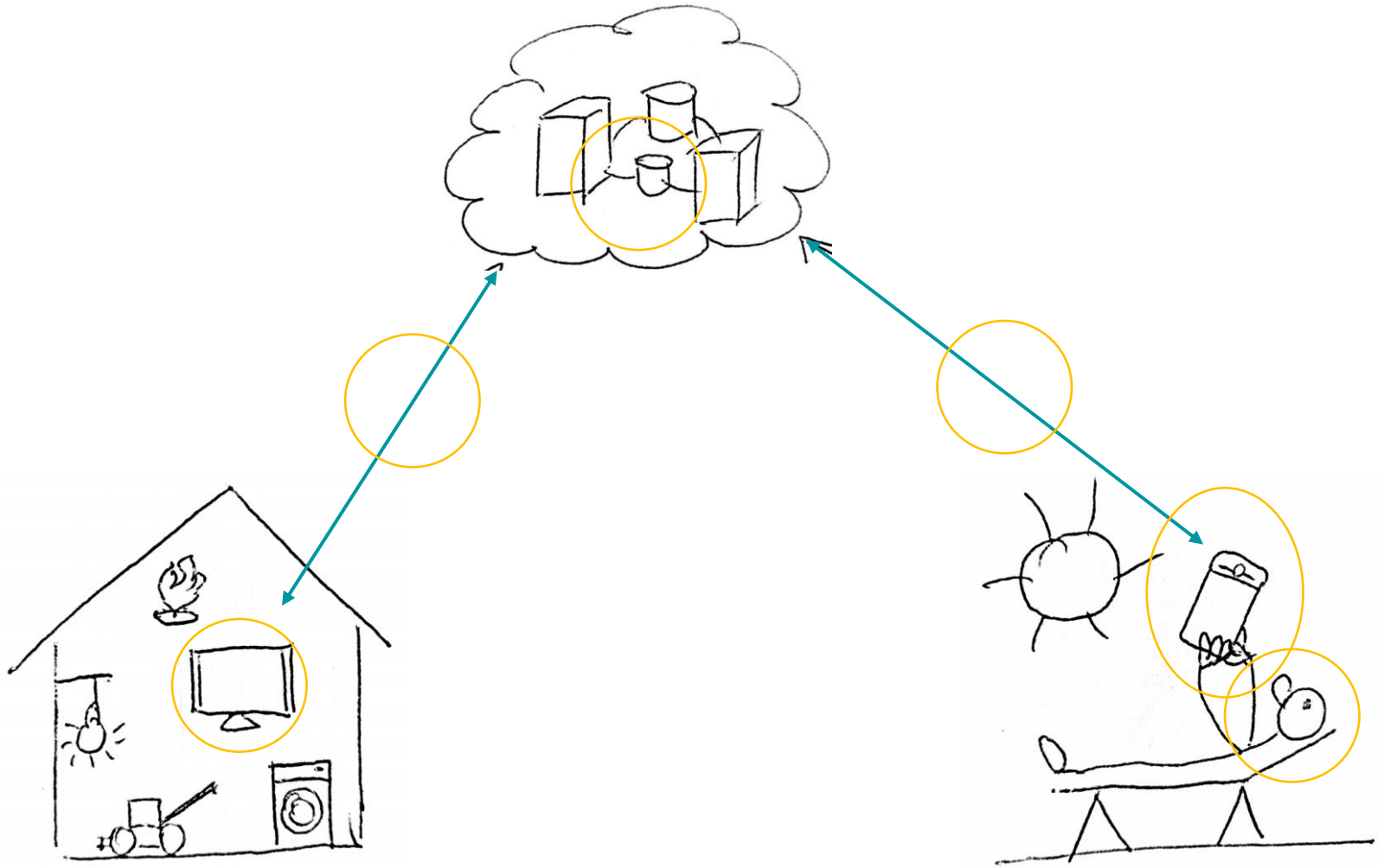




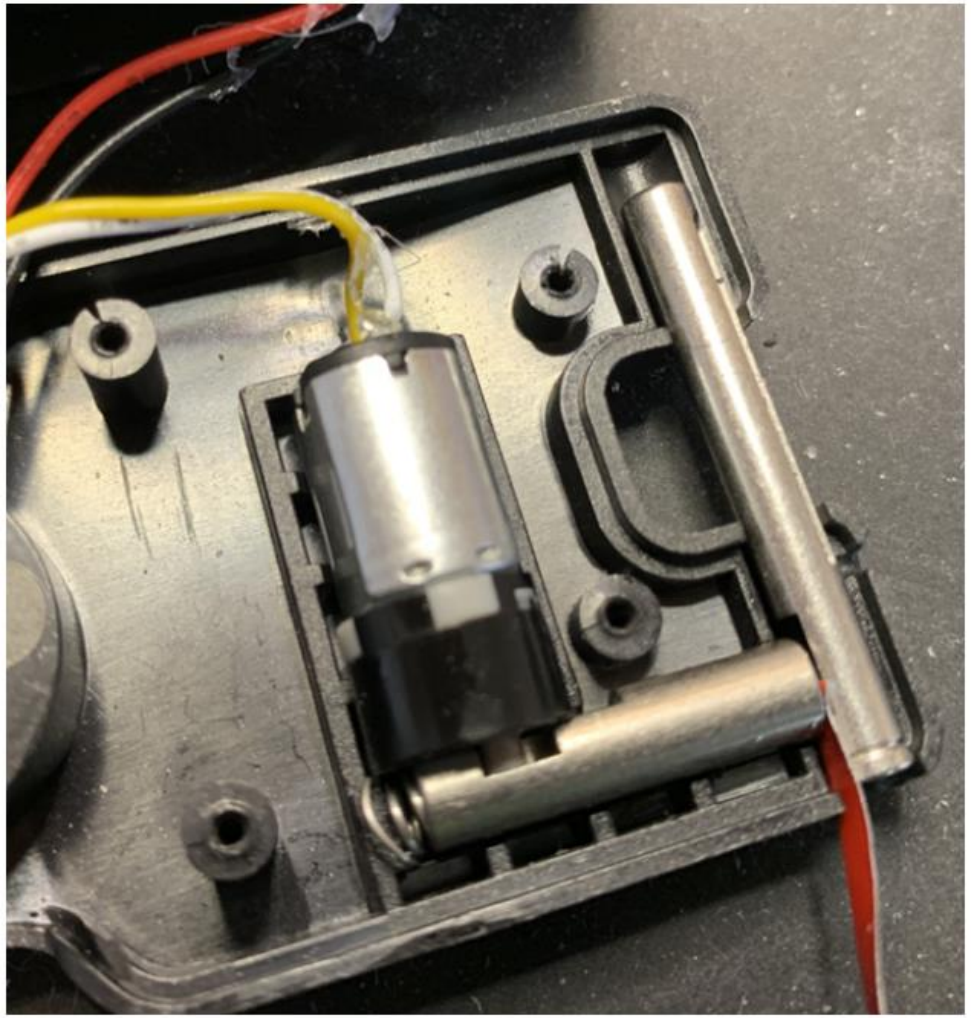




IOT – Internet of Things




CELL
MATE
CELL
MATE



https://www.pentestpartners.com/security-blog/smart-male-chastity-lock-cock-up/

Děkuji za pozornost

igor.hak@eset.cz

Digital Security
Progress. Protected.