



Phishingator

aneb cvičný phishing „nejen“ na ZČU

Martin Šebela

WIRT CIV ZČU, FLAB CESNET

EurOpen 2022 – 31. 5. 2022

Phishingator



= **Systém pro rozesílání cvičných phishingových zpráv**

- Prvotní myšlenka „o phishingu“ po semestrální práci, navázala bakalářská práce
- Příklad **cvičného phishingu pro studenty ZČU:**

Od Stravovací viceprezident SKM <vice@zcu.cz>

Předmět **Obědové stipendium pro studenty**

Komu já <msebela@students.zcu.cz>

Vážený strávníku msebela,
díky grantu EU 167/7669077-6429CZ je možné se přihlásit k bezplatným objedům.

Přihlásit se zde: <https://zcu.webkdc.cz/?ha041d1>

Časový limit pro přihlašování je 16. 4. 2019

Bc. et Bc. Jan Hladový
Stravovací viceprezident
vice@skam.zcu.cz
+555 123 646 888
SKM, ZČU ve v Plzni



- Phishingator = **automatizovaný nástroj** pro rozesílání cvičných phishingů
- Praktický **doplněk** ke školení „kdykoliv a kdekoliv“
- **Cílené školení**
- Založeno na **dobrovolné registraci** k odběru **cvičného phishingu**
- **Zpětná vazba pro uživatele** o absolvování cvičného phishingu
- Vytváření vlastních **phishingových kampaní** = podvodný e-mail + podvodná stránka

Příklad cvičného phishingu



- Na základě **skutečného phishingu na mzdy** registrovaného několika univerzitami v ČR
- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku**:



Z pohledu administrátora



- Vytvoření **cvičného phishingu**

1. **Jméno odesílatele**

2. **E-mail odesílatele**

3. **Předmět**

4. **Parametrizované tělo e-mailu**

- Možnost personalizace

Phishingator v0.8

Systém pro rozesílání cvičných phishingových zpráv

msebel (administrátor) Změnit roli

Seznam e-m

Úvodní stránka

Kampaně

Podvodné e-mail

Podvodné stránky

Uživatelé

Skupiny

Podvodné e-mail

Tato sekce slouží k vytváření nových a správě dosud vytvořených podvodných e-mailů (phishingu), které jsou dále využívány v tzv. [kampaních](#). Stejně tak lze ke každému z podvodných e-mailů vložit indicii, které si bude moci příjemce po svém přihlášení do systému prohlédnout. Každý z e-mailů si lze rovněž prohlédnout v náhledu, který je již personalizován vůči přihlášenému uživateli. Podrobnější informace jsou k dispozici v dostupné [nápoověd](#).

Název

☐ Skrýt před správci testů

Název slouží pouze k identifikaci v rámci tohoto systému.

Jméno odesílatele (nepovinné)

1.

E-mail odesílatele

2.

Při nevyplnění bude použit e-mail odesílatele z následujícího pole, v opačném případě bude odesílatel uveden ve tvaru `Jméno <email@domain.tld>`.

Při použití proměnné `%recipient_email%` bude jako odesílatel uveden e-mail příjemce.

Předmět

3.

Tělo

4.

`- %url%`

`@ Západočeská univerzita v Plzni`

`---`

`Tento e-mail byl zkontrolován programem na viry.`

Proměnné

Pro vložení proměnné do těla e-mailu můžete kliknout na její název v následujícím seznamu:

- `%recipient_username%` – uživatelské jméno příjemce
- `%recipient_email%` – e-mail příjemce
- `%date_cz%` – datum, ve kterém dochází k odeslání e-mailu v českém formátu (11.03.2021)
- `%date_en%` – datum, ve kterém dochází k odeslání e-mailu ve formátu YYYY-MM-DD (2021-03-11)
- `%url%` – URL podvodné stránky svázané s e-mailem

V těle e-mailu lze používat proměnné, které budou při odeslání e-mailu nahrazeny zvoleným obsahem.

Náhled

Uložit změny

31. května 2022

Indicie k rozpoznání phishingu



Od: Západočeská univerzita <caitrin.engle@webzcu.cz>
Předmět: Kalendář plánu mezd 2021 je nyní k dispozici (důležitý)
Kalendář plánu mezd 2021 je nyní k dispozici:
- %url%
© Západočeská univerzita v Plzni

Tento e-mail byl zkontrolován programem na viry.

1. Náhled podvodného e-mailu se zvýrazněnými indiciemi

👁️ Náhled včetně indicií

Přehled indicií k této zprávě

Indicie (podezřelý řetězec)

%sender_email%

Nadpis

E-mail odesílatele

Popis (nepovinné)

E-mail odesílatele nemá se ZČU nic společného.

🗑️ Smazat

🔗 Uložit změny

Indicie (podezřelý řetězec)

%url%

Nadpis

Podezřelá URL

Popis (nepovinné)

Nejedná se o oficiální doménu ZCU.CZ, ale o snahu útočníka napodobit její název falešnou doménou WEBZCU.

🗑️ Smazat

🔗 Uložit změny

Indicie (podezřelý řetězec)

zkontrolován programem na viry

Nadpis

Tento text může připsat

Popis (nepovinné)

Neříká to nic o věrohodnosti e-mailu.

🗑️ Smazat

🔗 Uložit změny

2. Přidání indicií (typických znaků phishingu), na základě kterých bylo možné phishing rozpoznat

Vytvoření podvodné stránky



- Nákup vhodné, cvičné, phishingové **domény**
 - **zcu.cz** vs. **zzu.cz**, **webzcu.cz**, ...
- Nasměrování DNS domény na aplikaci Phishingator
- Vytvoření a vložení **HTML šablony** s podvodnou stránkou do aplikace Phishingator
- Případně vydání **certifikátu**
- Phishingator na stránku **umístí logo** na základě domovské organizace uživatele

MUNI

VYSOKÉ UČENÍ
TECHNICKÉ
V BRNĚ

Uživatelské jméno

Heslo

Přihlásit

Vaše uživatelské jméno:

Heslo:

Přihlásit

Kampaň

- **Phishingová kampaň se skládá z:**
 - **phishingový e-mail**
 - **podvodná stránka**
 - **co se stane na podvodné stránce po odeslání formuláře**
 - **od kdy, do kdy**
 - **čas rozesílání**
 - **příjemci**

Phishingator v0.8

Úvodní stránka

Kampaně

Podvodné e-maily

Podvodné stránky

Uživatelé

Skupiny

Systém pro rozesílání cvičných phishingových zpráv

msebel (administrátor)

Změnit roli

[→ Odhlásit]

Kampaně

Tato sekce slouží k vytváření nových a správě dosud vytvořených kampaní. Každá z kampaní je svázána se zvoleným **podvodným e-mailem** a **podvodnou webovou stránkou**, na kterou se příjemce e-mailu dostane právě z obsahu tohoto e-mailu (pokud bude následovat odkazy v něm uvedené). Podrobnější informace jsou k dispozici v dostupné **nápovědě**.

Název

Spear phishing na mzdy (dobrovolní zaměstnanci + CIV)

Název slouží pouze k identifikaci v rámci tohoto systému.

Rozesílaný podvodný e-mail

Spear phishing podobný tomu z MUNI (CRP projekt)

Podvodný e-mail, který účastníci kampaně dostanou do svých e-mailových schránek a ze kterého se budou moci dostat na podvodnou stránku.

Podvodná webová stránka přístupná z e-mailu

http://login.webzcu.cz – WebAuth ZČU, přihlášení (věrná kopie)

Podvodná stránka, na kterou se uživatel dostane z podvodného e-mailu.

Akce po odeslání formuláře

Informace, že jde o test

Jedná se o akci, která se stane tehdy, když uživatel na stránce vyplní formulář a klikne na tlačítko pro jeho odeslání.

Start kampaně

10. 03. 2021

Udává, od kdy bude přístupná podvodná stránka a zároveň je to den, kdy započne odesílání e-mailů zvoleným příjemcům.

Spustit rozesílání e-mailů v čase

11:30

Určuje, od jakého času systém začne rozesílat zvoleným příjemcům vybraný e-mail.

Ukončení kampaně (včetně)

11. 03. 2021

Určuje, do jakého data bude kampaň aktivní, tzn. do jakého data budou sbírány výsledky a do jakého data bude přístupná zvolená podvodná stránka.

Uložit změny

Seznam účastníků kampaně

Celkem: 173

msebel@civ.zcu.cz

v.zcu.cz

.zcu.cz

zcu.cz

.zcu.cz

cu.cz

v.zcu.cz

zcu.cz

cu.cz

cu.cz

iv.zcu.cz

.zcu.cz

zcu.cz

iv.zcu.cz

.zcu.cz

.zcu.cz

v.zcu.cz

zcu.cz

iv.zcu.cz

cu.cz

iv.zcu.cz

Každý z příjemců musí být umístěn na samostatném řádku.

Vybrat příjemce

31. května 2022

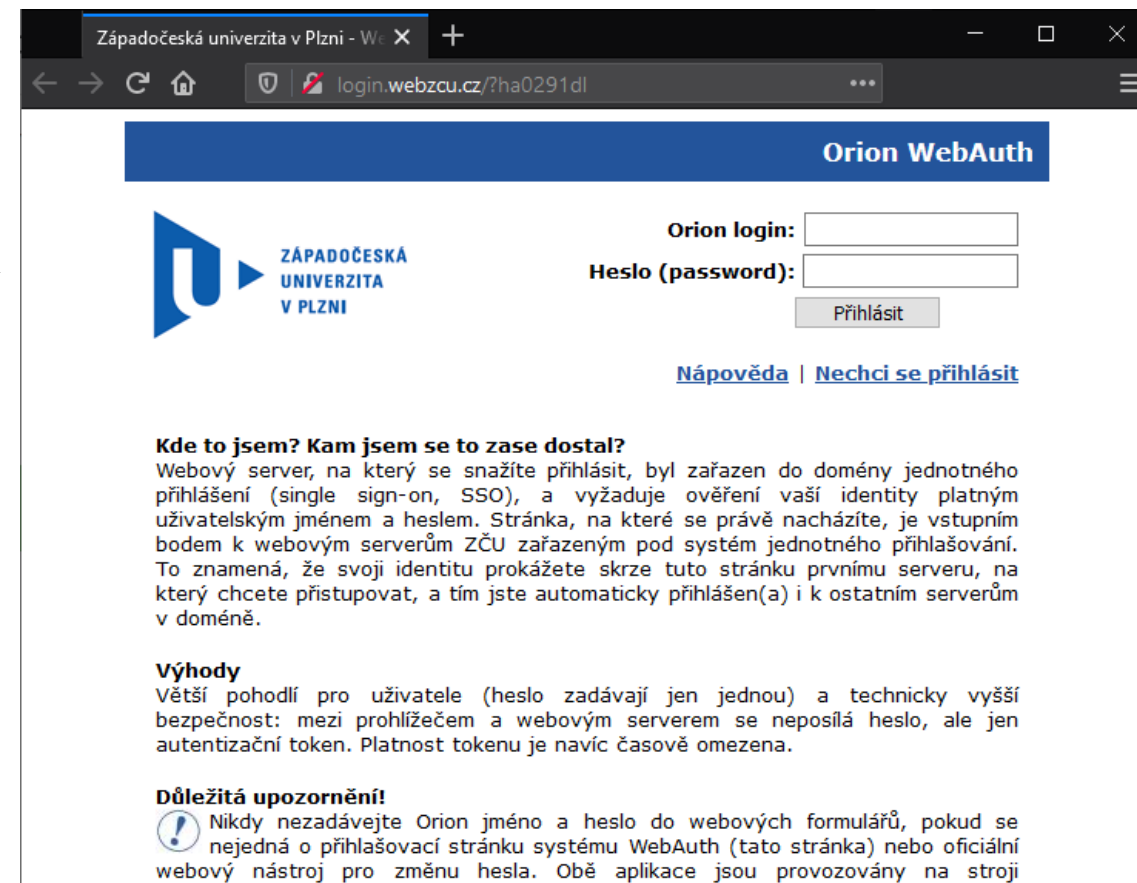
Phishingator aneb cvičný phishing „nejen“ na ZČU
EurOpen 2022

8 / 23

Z pohledu uživatele



- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku**



Po zadání údajů...

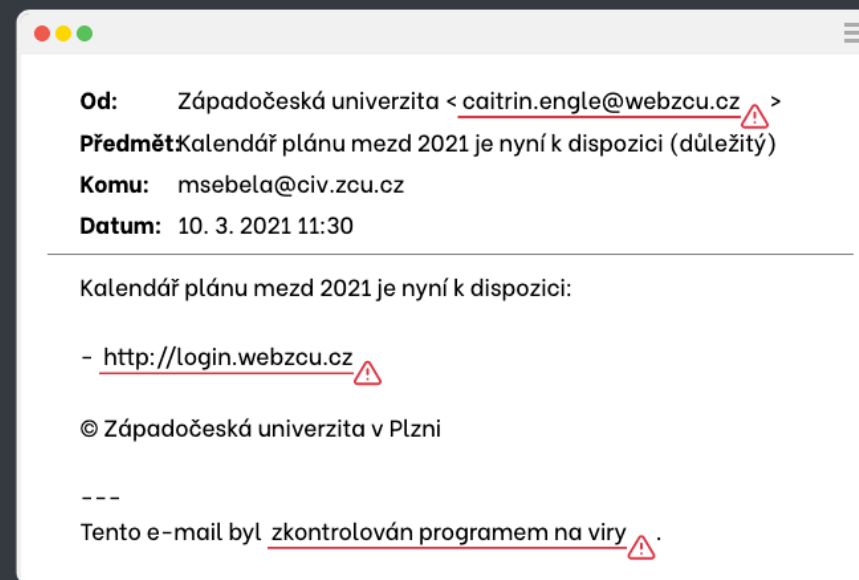
- Po vyplnění údajů na podvodné stránce:
 - Zobrazí se **podvodný e-mail**
 - Včetně indicií** pro jeho rozpoznání
- Okamžitá zpětná vazba** pro uživatele, kteří do formuláře cokoliv vyplnili

Právě jste absolvovali **cvičný phishing**

Děkujeme, že máte zájem **vzdělávat se** v oblasti **phishingu**. Jakékoliv **změny** včetně nastavení **limitu** **cvičných e-mailů** můžete provést po přihlášení do Phishingatoru.

VÍCE INFORMACÍ...

Jak bylo možné **phishing** rozpoznat z **e-mailu**



1. indicie E-mail odesílatele

E-mail odesílatele nemá se ZČU nic společného.

^ Označit

2. indicie Podezřelá URL

Nejedná se o oficiální doménu ZCU.CZ, ale o snahu útočníka napodobit její název falešnou doménou WEBZCU.CZ.

^ Označit

3. indicie Tento text může připisat každý

Neříká to nic o věrohodnosti e-mailu.

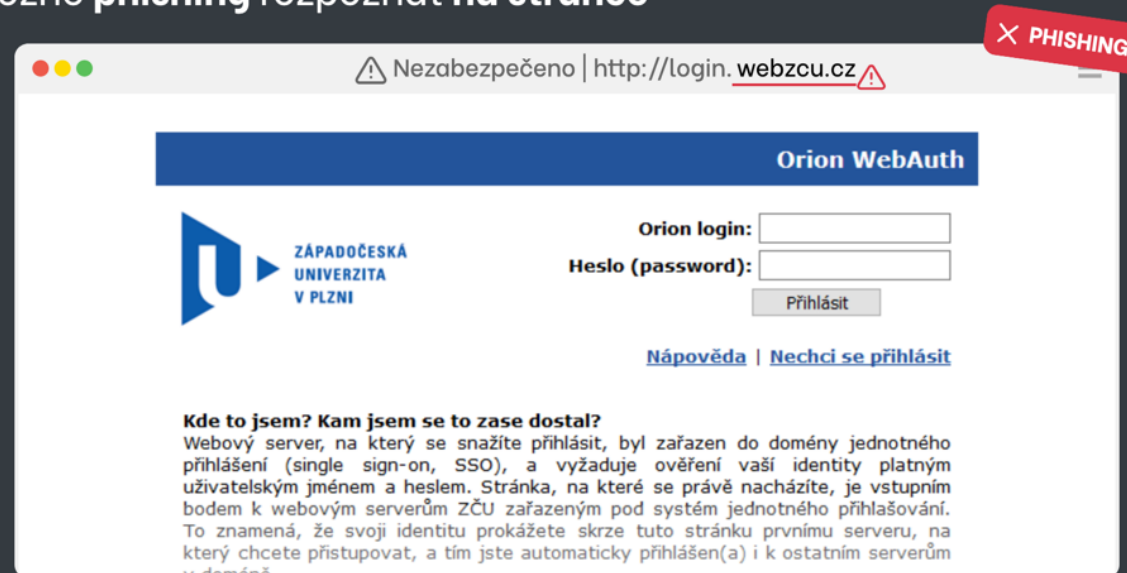
^ Označit

Po zadání údajů...



- Kromě indicií na podvodný e-mail jsou zobrazeny i **indicie k rozpoznání podvodné stránky**
- Upozornění na **URL**, chybějící **HTTPS**

Jak bylo možné **phishing** rozpoznat na stránce



1. indicie Špatná adresa stránky

Snaha o napodobení adresy stránky – je třeba sledovat adresu webu až do jejího konce. Nejedná se o oficiální doménu ZCU.CZ, ale o snahu útočníka napodobit její název falešnou doménou WEBZCU.CZ.

^ Označit

2. indicie Nezabezpečená stránka

Adresa stránky začíná zkratkou **HTTP** místo zabezpečeného protokolu **HTTPS**. Také může být vedle adresy vidět popisek „ **Nezabezpečeno**“ – to znamená, že všechno, co na webu děláte a zadáte, může kdokoliv sledovat.

Po ukončení phishingové kampaně



- **Notifikace** (zpětná vazba) **pro všechny příjemce**
- Především pro uživatele:
 - kteří se na stránku s indiciemi vůbec **nedostali** (cvičný phishing rozpoznali a obratem smazali)
 - kteří se do Phishingatoru registrovali, ale už na to **zapomněli**

Phishingator · Cvičný phishing z 10. 3. 2021

Čtvrtek, Březen 11, 2021 09:00 CET



Phishingator noreply@phishingator.zcu.cz

Komu

msebela@civ.zcu.cz

Automatická notifikace systému Phishingator

Dne 10. 3. 2021 (15:30) Vám byl odeslán e-mail "Kalendář plánu mezd 2021 je nyní k dispozici (důležitý)". Jednalo se o cvičný phishing (podvodnou zprávu) s typickými znaky, které útočníci používají při snaze získat Vaše heslo, číslo platební karty apod.

Gratulujeme, v testu jste obstáli :)

E-mail včetně indicií pro jeho rozpoznání si můžete prohlédnout zde:
<https://phishingator.zcu.cz/phishing/ha0301dl>

Děkujeme, že máte zájem vzdělávat se v oblasti phishingu.

Váš zbývající počet cvičných phishingových zpráv: nenastaven
Změnu můžete provést po přihlášení na:
<https://phishingator.zcu.cz>

Z pohledu uživatele



- **Přístupné všem** ze ZČU
- Možnost se **dobrovolně přihlásit k odebírání**
 - Limit zasílaných cvičných e-mailů
- **Historie** přijatých e-mailů
- **Reakce uživatele** na e-mail
- **Indicie k rozpoznání phishingu**

Phishingator v0.8

msebel (uživatel) Změnit roli ↕ ↗ Odhlásit

Úvodní stránka
Moje účast v programu
Přijaté phishingové e-maily

Moje účast v programu

[Nápověda](#)

Pro dobrovolné zapojení do programu nebo naopak odhlášení z programu stačí upravit možnosti v této sekci. Podrobnější informace jsou k dispozici v dostupné [nápovědě](#).

☒ **Ano, chci se dobrovolně přihlásit k odebírání cvičných phishingových zpráv**

To znamená, že několikrát do roka do mé e-mailové schránky dorazí e-mail, který bude obsahovat typické znaky phishingu a sociálního inženýrství. Na rozdíl od toho reálného mi ovšem ten cvičný nic neprovede ani neukradne.

☒ Omezit počet zpráv, které mi budou zaslány (nepovinné)

Zbývající počet cvičných phishingových zpráv, o které mám zájem

10

Po odeslání každé zprávy dojde ke snížení tohoto čísla. Po dosažení nuly nebude zaslána žádná další zpráva, dokud toto číslo opět nezvýšíte.

[Změnit mé nastavení](#)

Z pohledu administrátora – výsledky kampaně



- Všechny reakce příjemců:
 - bez reakce
 - návštěva podvodné stránky
 - vyplnění neplatných přihlašovacích údajů
 - vyplnění platných přihlašovacích údajů
- Možnost sledovat průběžné výsledky
- Data zadaná na podvodné stránce (anonymizováno)

Systém pro rozesílání cvičných phishingových zpráv

msebel (administrátor) Změnit roli [→ Odhlásit]

Kampaně

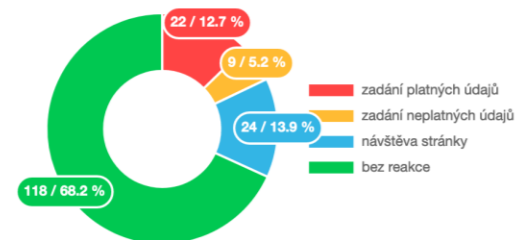
Seznam kampaní

Tato sekce slouží k vytváření nových a správě dosud vytvořených kampaní. Každá z kampaní je svázána se zvoleným [podvodným e-mailem](#) a [podvodnou webovou stránkou](#), na kterou se příjemce e-mailu dostane právě z obsahu tohoto e-mailu (pokud bude následovat odkazy v něm uvedené). Podrobnější informace jsou k dispozici v dostupné [návodě](#).

Základní informace

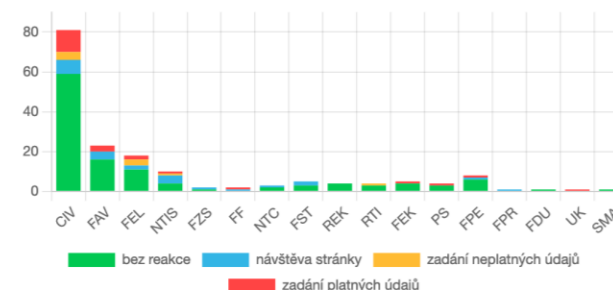
Název	Přidáno	Přidal	Podvodný e-mail	Podvodná stránka	URL podvodné stránky	Odesláno e-mailů	Spuštění rozesílání	Aktivní od	Aktivní do	RT kampaně		
Spear phishing na mzdy (dobrovolní zaměstnanci + CIV)	10. 3. 2021	msebel	Spear phishing podobný tomu z MUNI (CRP projekt)	 Náhled	WebAuth ZČU, přihlášení (věrná kopie)	http://login.webzcu.cz	 Náhled	173/173	každý den od 11:30	 10. 3. 2021	 11. 3. 2021	–

Konečné akce uživatelů v kampani

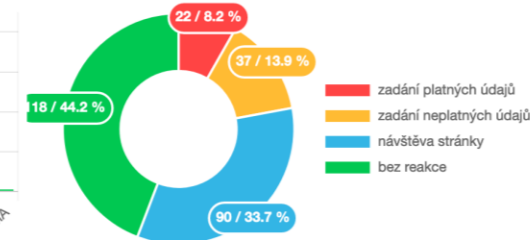


Tabulka konečných akcí

Konečné akce v kampani dle skupiny



Provedené akce v kampani



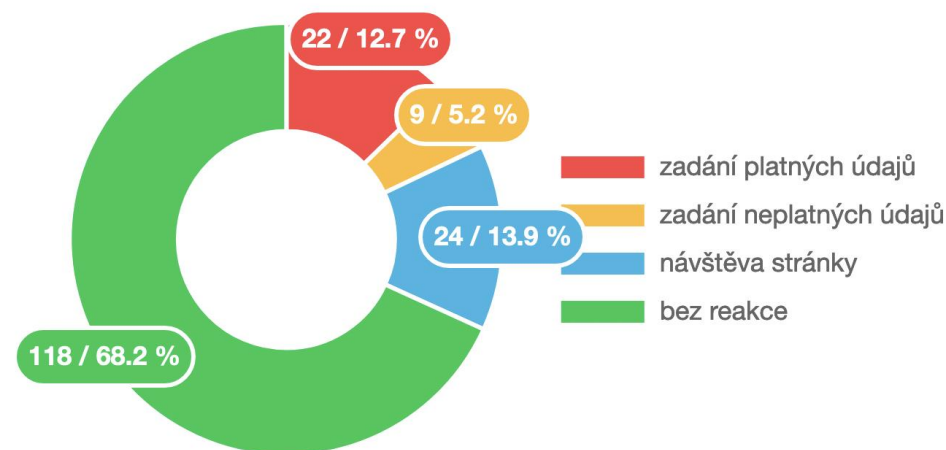
Tabulka všech provedených akcí

Cvičný phishing na mzdy



- **Rozesláno 173** vybraným **zaměstnancům**
 - napříč fakultami a dalšími součástmi ZČU
 - získáno **22 platných identit** během 2 hodin
- **Všechny reakce příjemců:**
 - **bez reakce (118)**
 - **návštěva podvodné stránky (24)**
 - vyplnění **neplatných** přihlašovacích údajů **(9)**
 - vyplnění **platných** přihlašovacích údajů **(22)**
- Stejná kampaň pro dalších **70** zaměstnanců

Konečné akce uživatelů v kampani



Časová osa cvičné phishingové kampaně



- **173** odeslaných e-mailů

1. **11:30** – odeslání cvičného phishingu
2. **11:31** – první návštěva podvodné stránky
3. **11:31** – první získaná identita
4. **11:35** – získáno 8 platných identit
5. **do 12:00** – získáno 15 platných identit

20	CIV	návštěva stránky	10. 3. 2021 11:32:52	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...
19	CIV	návštěva stránky	10. 3. 2021 11:32:40	88.100	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
18	FEL	návštěva stránky	10. 3. 2021 11:32:39	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
17	CIV	návštěva stránky	10. 3. 2021 11:32:36	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...
16	CIV	zadání platných údajů	10. 3. 2021 11:32:13	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome... {"username":
15	KMA	zadání platných údajů	10. 3. 2021 11:32:12	88.100	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/... {"username":
14	KIV	návštěva stránky	10. 3. 2021 11:32:09	89.102	Mozilla/5.0 (Linux; Android 10; YAL-L41) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.86 Mobile Safari/537.36
13	FZS	návštěva stránky	10. 3. 2021 11:32:04	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
12	FPE	zadání platných údajů	10. 3. 2021 11:32:00	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/... {"username":
11	KMA	návštěva stránky	10. 3. 2021 11:31:57	88.100	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Mobile/...
10	CIV	návštěva stránky	10. 3. 2021 11:31:56	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36
9	FPE	návštěva stránky	10. 3. 2021 11:31:51	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.72 Safari/537.36 Edg/...
8	CIV	zadání platných údajů	10. 3. 2021 11:31:50	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP... {"username":
7	NTIS	návštěva stránky	10. 3. 2021 11:31:49	147.228	Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
6	CIV	návštěva stránky	10. 3. 2021 11:31:48	212.11	Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/13.2 Chrome...
5	CIV	zadání platných údajů	10. 3. 2021 11:31:47	89.102	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36 {"username":
4	CIV	návštěva stránky	10. 3. 2021 11:31:42	147.228	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 OP...
3	CIV	návštěva stránky	10. 3. 2021 11:31:39	89.102	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36
2	CIV	zadání neplatných údajů	10. 3. 2021 11:31:10	147.228	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0 {"username":
1	CIV	návštěva stránky	10. 3. 2021 11:31:04	147.228	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0

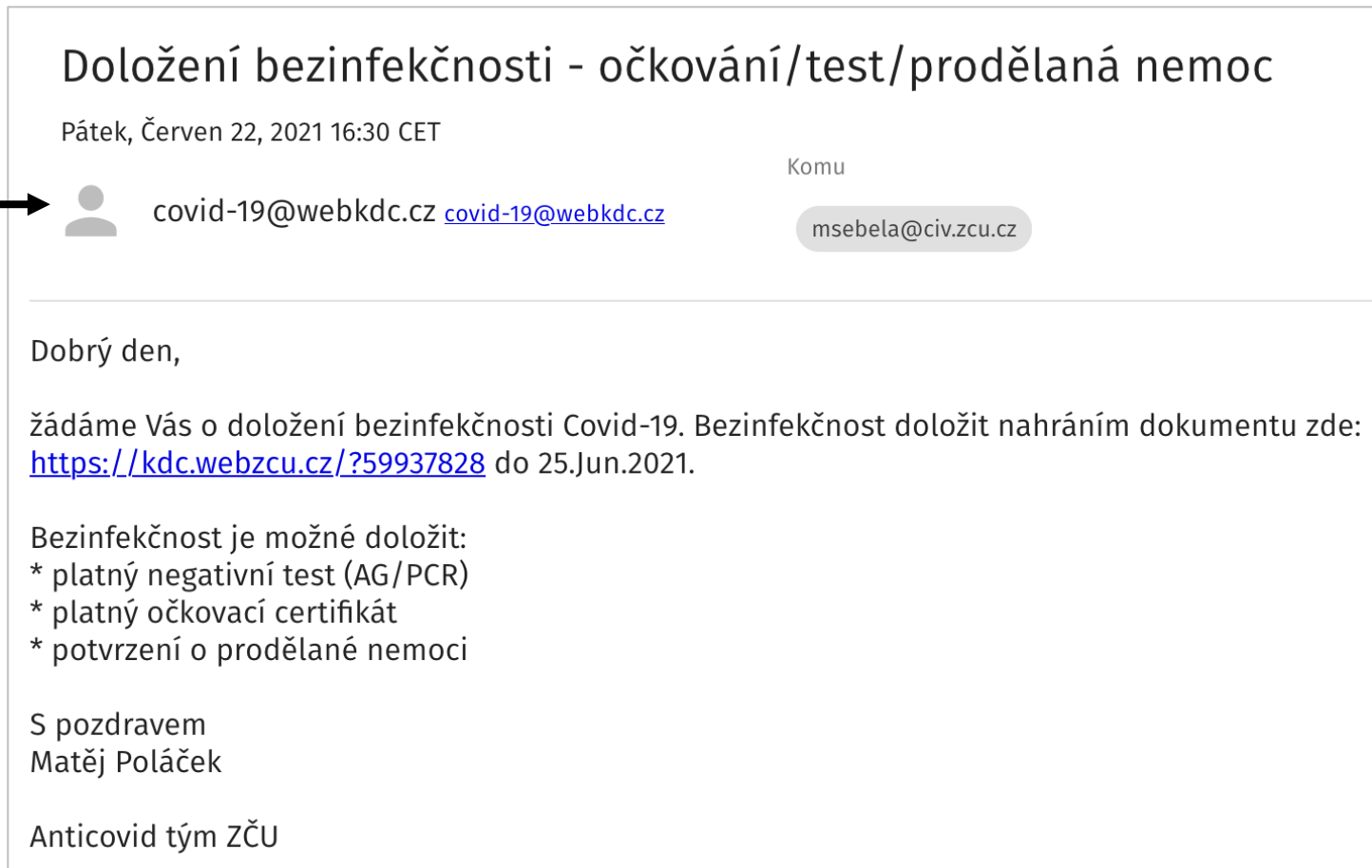
Cvičný phishing na doložení bezinfekčnosti



- **Podvodný e-mail** odeslaný z Phishingatoru s odkazem na **podvodnou stránku**

- Odesílatel `covid-19@webkdc.cz`

- Odkaz na stránku `https://kdc.webzcu.cz`



Cvičný phishing na doložení bezinfekčnosti



- **Rozesláno 112** vybraným **zaměstnancům**

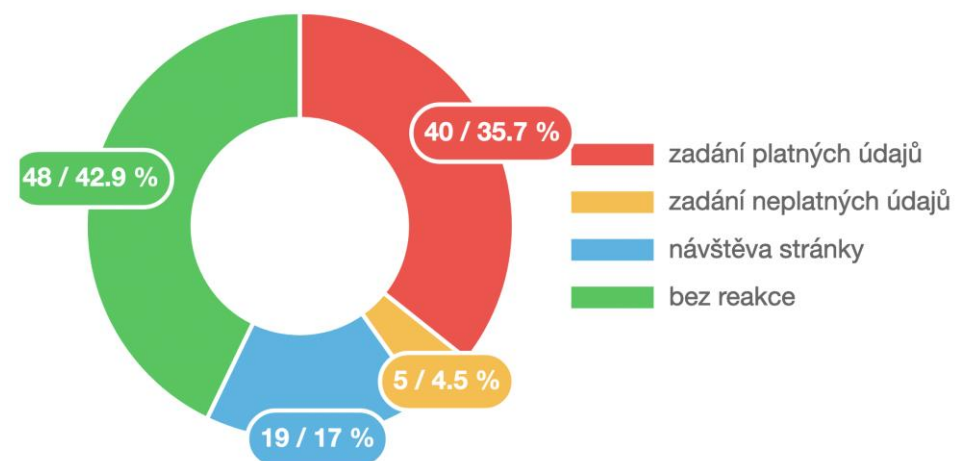
- získáno **40 platných identit**
- platné heslo zadáno **176x**

- **Všechny reakce** příjemců:

- **bez reakce (48)**
- **návštěva podvodné stránky (19)**
- vyplnění **neplatných** přihlašovacích údajů **(5)**
- vyplnění **platných** přihlašovacích údajů **(40)**

- Podobný výsledek u **cvičného phishingu** na **elektronický výplatní lístek**

Konečné akce uživatelů v kampani



Cvičný phishing na doložení bezinfekčnosti



- Nezobrazována stránka s indiciemi
- Odesílateli cvičného phishingu dorazilo **12 odpovědí**

Dobrý den, **certifikát Vám zasílám v příloze**, protože na Vámi uvedený odkaz se nelze přihlásit přes můj orion přístup. Máte tam zřejmě nějaké jiné přihlašování, které jste mi zatím nezaslali.

POZN: **Ani můj kolega se tam nedokázal přihlásit**, takže to asi bude problém pro všechny. ...

Dobrý den
Odkaz nejde otevřít,
zůstává stále na
přihlašovací obrazovce
**Certifikát Vám posílám
proto zde v příloze.**
S pozdravem ...

Dobrý večer, Od pátka se
tam nemůžu přihlásit.
Posílám to v emailu. ...

EU Digital
COVID Certificate

Certifikát EU
COVID-19



**POTVRZENÍ O ABSOLVOVÁNÍ TESTU NA
PRŮKAZ PŘÍTOMNOSTI AG SARS-COV-2**

POTVRZUJI, ŽE

Cvičný phishing na doložení bezinfekčnosti



- Nezobrazována stránka s indiciemi
- Odesílateli cvičného phishingu dorazilo **12 odpovědí**

Dobrý den,

nerad bych poskytoval osobní údaje, **když mám podezření, že se může jednat o "podvodný email"**.
Vaší osobu zčů **telefonní seznam nezná**, proto bych Vás chtěl požádat o prokázání, že se jedná o oficiální požadavek mého zaměstnavatele. ...

EU Digital
COVID Certificate

Certifikát EU
COVID-19



**POTVRZENÍ O ABSOLVOVÁNÍ TESTU NA
PRŮKAZ PŘÍTOMNOSTI AG SARS-COV-2**

POTVRZUJI, ŽE

Časová osa cvičné phishingové kampaně



- 112 odeslaných e-mailů

1. 16:30 – odeslání cvičného phishingu
2. 16:31 – první návštěva podvodné stránky
3. 16:31 – první získaná identita
4. 22:23 – získáno 12 platných identit

⋮



20		RTI	zadání platných údajů	22. 6. 2021 16:44:46	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
19		RTI	návštěva stránky	22. 6. 2021 16:44:43	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
18		KKS	návštěva stránky	22. 6. 2021 16:42:07	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
17		RTI	zadání platných údajů	22. 6. 2021 16:37:33	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
16		RTI	návštěva stránky	22. 6. 2021 16:37:26	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
15		RTI	zadání platných údajů	22. 6. 2021 16:37:02	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
14		RTI	zadání platných údajů	22. 6. 2021 16:36:53	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
13		RTI	návštěva stránky	22. 6. 2021 16:36:42	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
12		RTI	zadání platných údajů	22. 6. 2021 16:36:36	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
11		RTI	zadání platných údajů	22. 6. 2021 16:36:04	46.13		Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36	Phishing
10		RTI	zadání platných údajů	22. 6. 2021 16				Phishing
9		RTI	návštěva stránky	22. 6. 2021 16				Phishing
8		RTI	zadání neplatných údajů	22. 6. 2021 16				Phishing
7		RTI	návštěva stránky	22. 6. 2021 16				Phishing
6		RTI	návštěva stránky	22. 6. 2021 16				Phishing
5		RTI	zadání neplatných údajů	22. 6. 2021 16:32:28	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0	Phishing
4		RTI	zadání platných údajů	22. 6. 2021 16:32:03	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0	Phishing
3		RTI	zadání platných údajů	22. 6. 2021 16:31:54	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0	Phishing
2		RTI	návštěva stránky	22. 6. 2021 16:31:47	147.228		Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0	Phishing
1		RTI	návštěva stránky	22. 6. 2021 16:31:18	37.48		Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.1 Mobile/15E148...	Phishing

{"username":"achjozasemamjitnaskoleni?","passw" →



- Od **konce září 2022 bude možné nasadit** Phishingator i v jiných institucích
- Nabízeno v rámci **služeb bezpečnosti CESNET** – sluzby@cesnet.cz
- Režimy:
 - 1)** instituce si vše řeší sama (nasazení, provoz, phishingové kampaně)
 - 2)** CESNET řeší nasazení a provoz, kampaně vytváří instituce
 - 3)** CESNET řeší vše – nasazení, provoz i vytváření kampaní



- **Cílem** je uživatele **vzdělat** a ukázat na **nebezpečí phishingu**
- Nenásilné **poučení** pro uživatele
- **ZČU** má vlastní instanci pro **všechny své uživatele**
 - dobrovolné zapojení uživatelů ZČU
 - limit přijatých cvičných phishingů
- **CESNET** umožní a pomůže s nasazením a provozem Phishingatoru i jinde
 - **konec září 2022** – zájem pište na sluzby@cesnet.cz

Dotazy



Martin Šebela

msebela@civ.zcu.cz

WIRT CIV ZČU, FLAB CESNET