



Phishingator

Cvičný phishing nejen na českých univerzitách

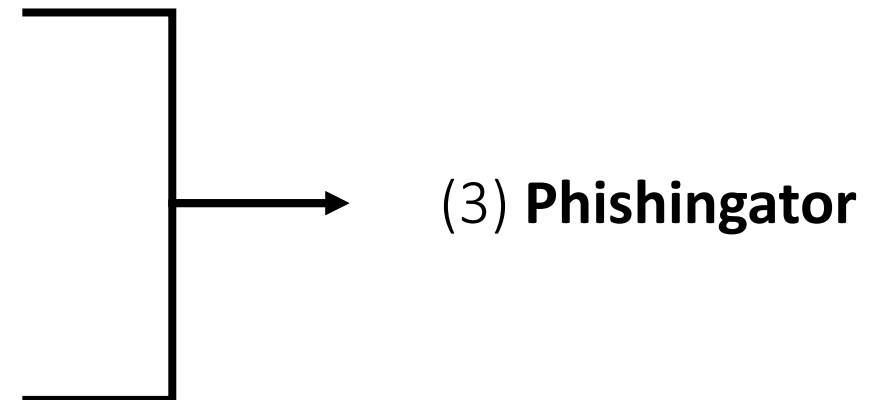
Martin Šebela – CESNET FLAB

31. května 2023

K čemu Phishingator?



- **Bezpečnostní riziko phishingu**
 - Prozrazení přístupových údajů
 - Potřeba vzdělaného uživatele
 - Propracovanější techniky útočníků
- (1) **Testy sociálního inženýrství** (FLAB CESNET)
 - Služba na klíč
 - Teoretické i praktické školení uživatelů
 - Závěrečná zpráva, prezentace výsledků
- (2) **Vlastní realizace** v organizaci
 - Teoretické školení – snadné
 - Praktický test – komplikovanější

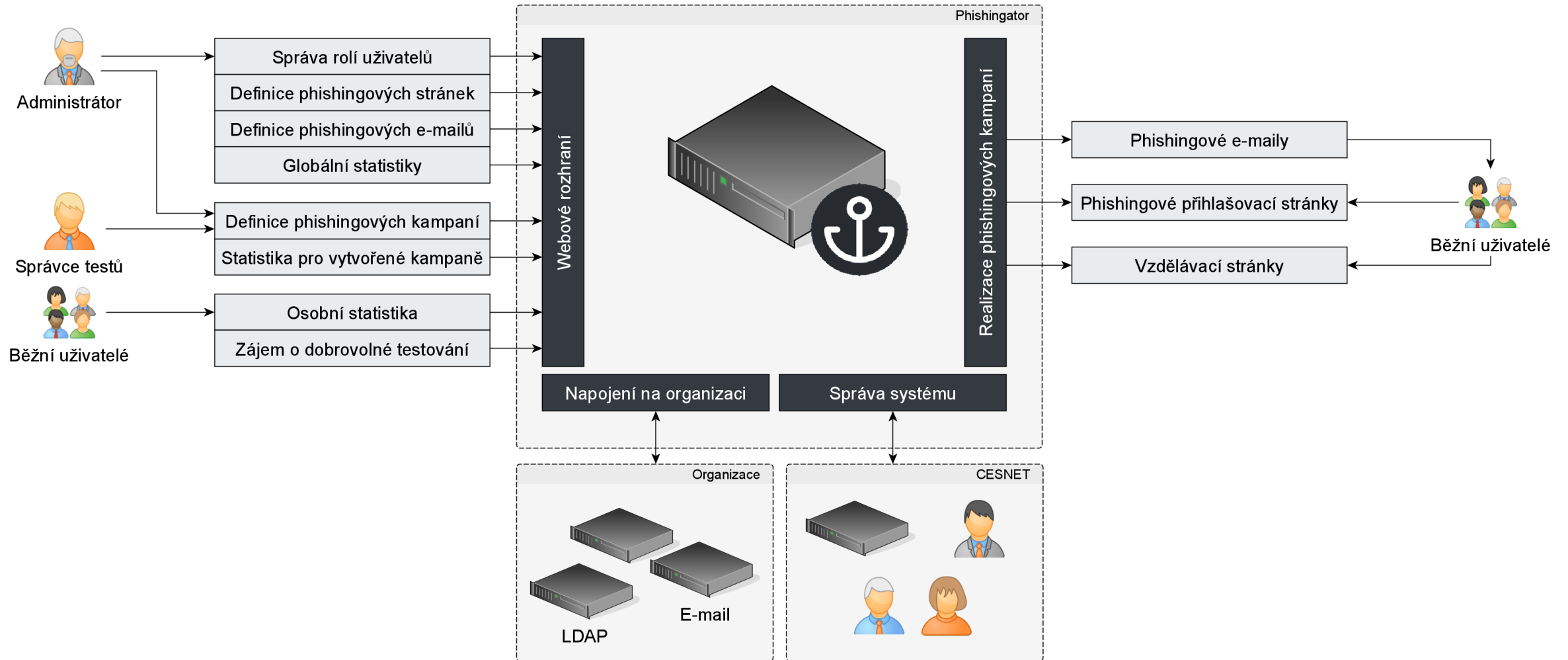




= Webová aplikace pro automatizované **rozesílání cvičných phishingových zpráv**

- Původně **bakalářská práce na ZČU (2019)**, nyní OpenSource
- **CESNET poskytuje formou Software as a Service**
 - Technicky se nemusíte o nic starat
 - Phishingator napojíme na Vaši organizaci
 - Každá organizace = **vlastní instance Phishingatoru**
- Praktický doplněk ke školení „kdykoliv a kdekoliv“
 - Přímá **konfrontace** s phishingem
 - **Cílené školení** uživatelů
- **Zpětná vazba pro uživatele** o absolvování cvičného phishingu

Phishingator

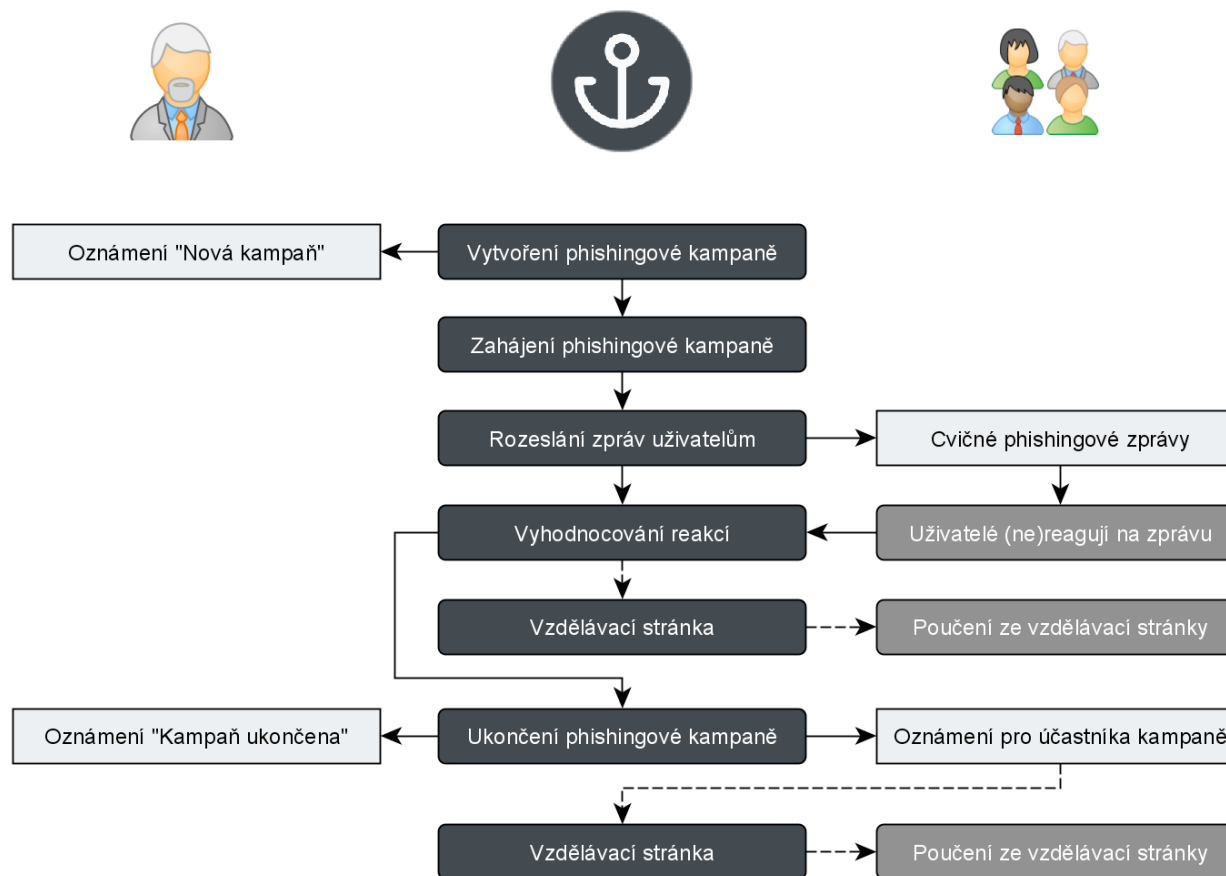


Průběh phishingové kampaně



- **Phishingová kampaň** = podvodný e-mail + podvodná stránka

1. Vytvoření **e-mailu** a **indicií**
2. Nákup podvodné **domény**
3. Vytvoření **podvodné stránky** (šablona + URL)
4. Rozeslání e-mailů **konkrétním příjemcům**
5. Sledování **reakcí příjemců**
6. Automatická **zpětná vazba pro příjemce**



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**:

Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)

Středa, Leden 18, 2023 21:45 CET

 CESNET mzdy@cesnet.cz

Komu

Martin.Sebela@cesnet.cz

Kalendář plánu mezd 2023 je nyní k dispozici:

- <https://cesnet.cz/?5615479>

© CESNET, z. s. p. o.

Tento e-mail byl zkontrolován programem na viry.

Z pohledu administrátora – vytvoření phishingu



- Vytvoření **cvičného podvodného e-mailu**

1. **Jméno odesílatele**
2. **E-mail odesílatele**
3. **Předmět**
4. **Parametrizované tělo e-mailu**
 - Možnost personalizace

Phishingator v1.2 Systém pro rozesílání cvičných phishingových zpráv Martin.Sebela administrátor [→ Odhlásit]

Podvodné e-maily

Tato sekce slouží k vytváření nových a správě dosud vytvořených podvodných e-mailů (phishingu), které jsou dále využívány v tzv. **kampaních**. Ke každému z podvodných e-mailů lze navíc vložit indicie, které jsou uživateli zobrazeny při podlehnutí phishingu, případně po ukončení kampaně. Každý z e-mailů si lze rovněž prohlédnout v náhledu, který je již personalizován vůči přihlášenému uživateli.

Skrýt před správci testů
E-mail uvidí a mohou rozesílat pouze administrátoři.

Název:

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.**

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 (18. 1. 2023)
%date_en% – datum, ve kterém dochází k odeslání e-mailu ve formátu YYYY-MM-DD (2023-01-18)
%url% – URL podvodné stránky svázané s e-mailem

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

Vyplnění indicií k rozpoznání phishingu



Od: CESNET <mzdy@csenet.cz>
Předmět: **Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)**
Kalendář plánu mezd 2023 je nyní k dispozici:

- [%url%](#) ⚠

© CESNET, z. s. p. o.

Tento e-mail byl [zkontrolován programem na viry](#) ⚠.

1. Náhled podvodného e-mailu s červeně zvýrazněnými indiciemi

👁️ Náhled včetně indicií

Indicie (3) k rozpoznání tohoto phishingu

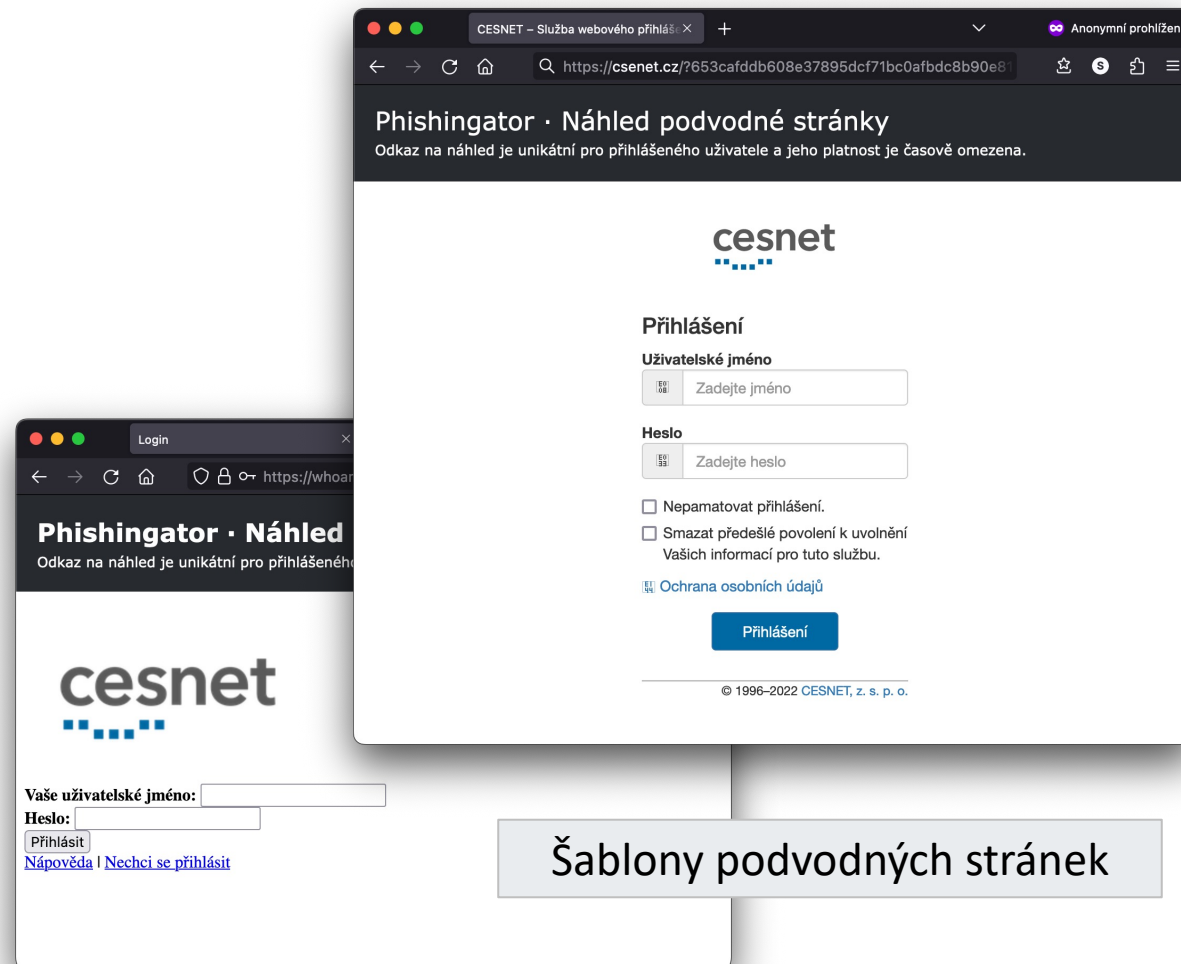
Indicie (podezřelý řetězec)	Nadpis	Popis (nepovinné)	
<input type="text" value="%sender_email%"/>	<input type="text" value="E-mail odesílatele"/>	<input type="text" value="E-mail odesílatele nemá s organizací CESNET nic společného."/>	<input type="button" value="Smazat"/> <input type="button" value="Uložit změny"/>
<input type="text" value="%url%"/>	<input type="text" value="Podezřelá URL"/>	<input type="text" value="Nejedná se o oficiální doménu CESNET.CZ, ale o snahu útočnicka napodobit její"/>	<input type="button" value="Smazat"/> <input type="button" value="Uložit změny"/>
<input type="text" value="zkontrolován programem na vir"/>	<input type="text" value="Tento text může připsat každý"/>	<input type="text" value="Neříká to nic o věrohodnosti e-mailu."/>	<input type="button" value="Smazat"/> <input type="button" value="Uložit změny"/>

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

Vytvoření podvodné stránky



- Nákup cvičné, phishingové **domény**, kde bude hostována podvodná stránka
 - Překlepy, snaha napodobit název organizace
 - Např. pro CESNET:
cesnet.cz vs. **cse**net.cz, **oes**net.cz, ...
- Nasměrování **DNS** na Phishingator
- Vytvoření **HTML šablony** pro podvodnou stránkou
- Případně vydání **HTTPS certifikátu**
- Volba **URL adresy** (různé adresáře a parametry v adrese)



Kampaň

- Phishingová kampaň se skládá z:
 1. podvodný e-mail
 2. podvodná stránka
 3. co se stane po vyplnění formuláře na podvodné stránce
 4. od kdy, do kdy
 5. čas rozesílání
 6. příjemci

Phishingator v1.2 Systém pro rozesílání cvičných phishingových zpráv Martin.Sebela **administrátor** [→ Odhlásit]

Kampaně

Tato sekce slouží k vytváření nových a správě dosud vytvořených phishingových kampaní. Každá kampaň 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).

Název Číslo lístku s kampaní (nepovinné) Seznam účastníků kampaně Celkem: 2

Kalendář plánu mezd Číslo lístku (ticketu) v RT systému ohledně vytvoření phishingové kampaně.

Rozesílaný podvodný e-mail 1. Náhled

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 2. Náhled

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

Akce po odeslání formuláře 3. Náhled

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

Start kampaně Spustit rozesílání e-mailů v čase 5.

18. 01. 2023 21:30

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

Ukončení kampaně (včetně) 4.

18. 01. 2023

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

Vybrat příjemce

Martin.Sebela@cesnet.cz
apadrta@cesnet.cz 6.

Přidat



- Pro administrátory

- Jak správně připravit cvičný phishing

- Pro uživatele

- Jak rozpoznat phishing
- Typické znaky

Systém pro rozesílání cvičných phishingových zpráv 🔍 Martin.Sebela **administrátor** ↕ Odhlásit

Jak připravit phishing 🔗 Nápověda

Podobně jako při psaní běžného e-mailu je nutné i při **vytváření cvičného podvodného e-mailu** pamatovat na určité **zásady**. Cílem je vždy sestavit cvičný podvodný e-mail, který uživatele **naučí odhalovat** a zaměřovat se na **typické znaky a techniky** používané ve **phishingových e-mailech**.

1. Vymyslete téma

Mezi **vhodná témata** pro cvičné podvodné e-maily například patří:

- **různé notifikace**, které běžně přicházejí – vypršení hesla, žádost o sdílení online dokumentu, kontrola použití účtu z jiné lokality, nepřečtené zprávy apod.,
- **kontrola nebo potvrzení** údajů,
- **test nové aplikace**,
- **elektronické odsouhlasení** navýšení platu.

2. Zvolte obtížnost

Cvičný podvodný e-mail by měl být **přizpůsoben zkušenostem příjemců**:

- **začátečnickům** a neproškoleným je vhodné rozesílat **lehčí phishing** (s třemi a více jasnými indiciemi),
- **pokročilým uživatelům** je možné rozesílat složitější a cílenější **spear phishing**.

V každém cvičném podvodném e-mailu by se však měly vyskytnout **jasné indicie**, na základě kterých bylo možné phishing rozpoznat.

3. Vytvořte podvodnou stránku + Nová podvodná stránka

Volba **vzhledu** příslušné podvodné stránky a **použití URL** (domény) rovněž **ovlivňuje obtížnost**:

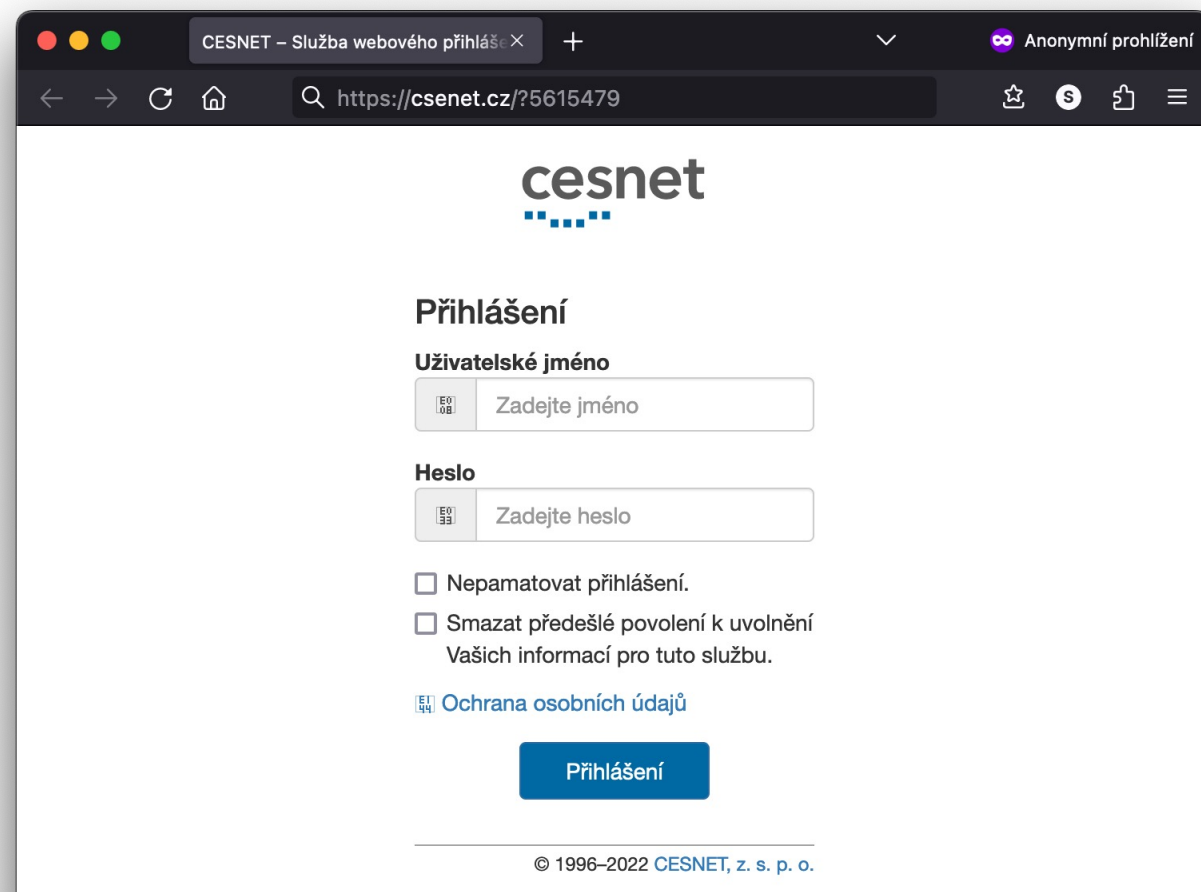
- Podvodné stránky se mohou **vizuálně shodovat** se skutečnou, pravou webovou stránku (např. s **přihlašovací stránkou** organizace), a to včetně **důvěryhodného HTTPS** certifikátu.
- **Podvodná doména** (tj. hostitel podvodné stránky) může ve svém názvu obsahovat například **nevýrazný překlep** oproti legitimní (správné) doméně nebo v ní mohou být například **tečky nahrazeny pomlčkou** (např. `login.cesnet.cz` vs. `login-cesnet.cz`).

Při použití podvodné stránky běžící na **nezabezpečeném protokolu HTTP** je možné, že data zadaná na podvodné stránce mohou být **odposlechnuta**. Uživatelům, kteří do takové podvodné stránky vyplnili platné přihlašovací údaje, by mělo být doporučeno **provést změnu hesla**.

Z pohledu uživatele



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



Po zadání údajů...

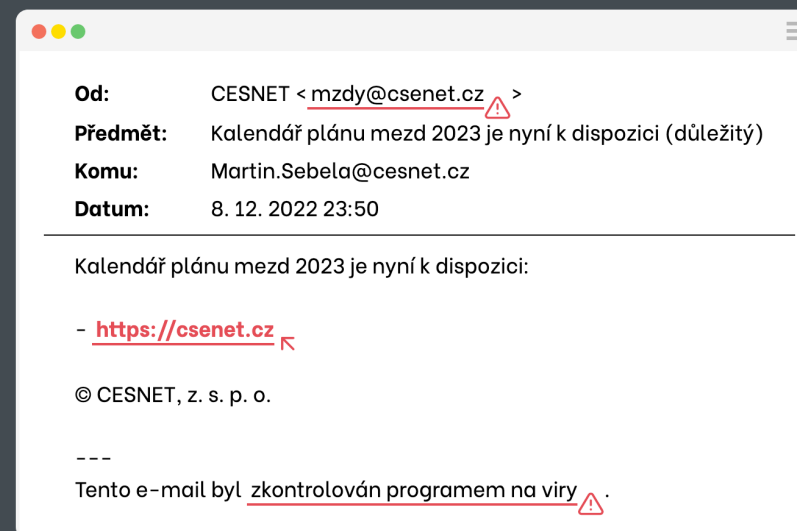
- Po **vyplnění formuláře** na podvodné stránce:
 - Zobrazí se **podvodný e-mail**
 - **Včetně indicií** pro jeho rozpoznání
- **Okamžitá zpětná vazba** pro uživatele, kteří do formuláře cokoliv vyplnili
 - „*Co jsem udělal špatně?*“

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 s organizací CESNET nic společného.

[^ Označit](#)

2. indicie Podezřelá URL

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

[^ Označit](#)

3. indicie Tento text může připisat každý

Neřiká to nic o věrohodnosti e-mailu.

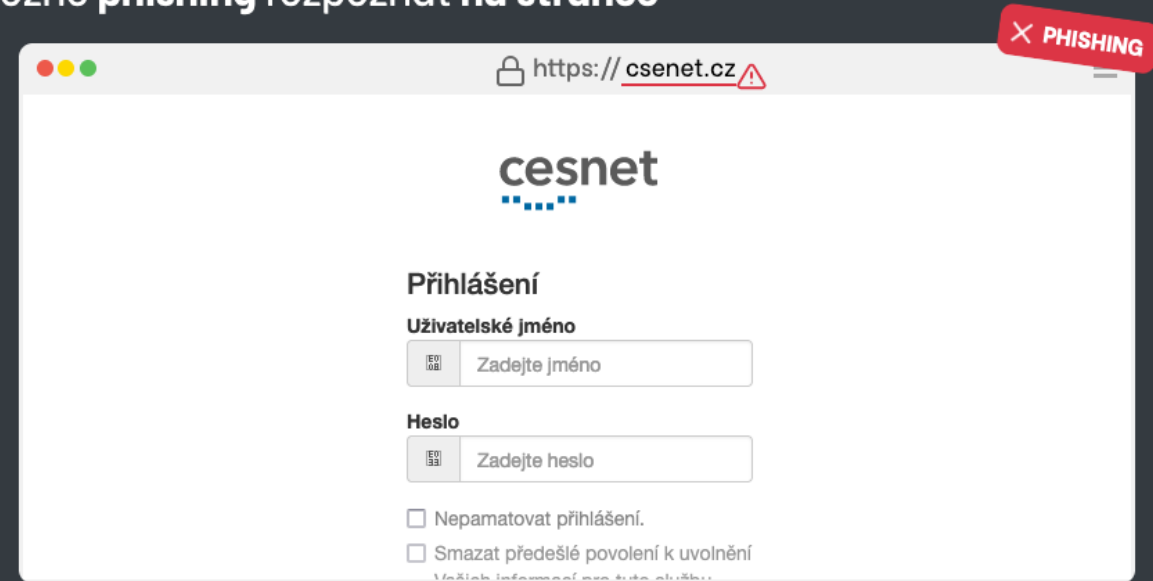
[^ Označit](#)

Po zadání údajů...



- Kromě indicií na podvodný e-mail jsou zobrazeny i **indicie k rozpoznání podvodné stránky**
- Upozornění na **nesprávnou URL, případně 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 CESNET.CZ, ale o snahu útočníka napodobit její název falešnou doménou.

^ Označit

Po ukončení phishingové kampaně



- **Zpětná vazba** (formou notifikace) 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 18. 1. 2023

Čtvrtek, Leden 19, 2023 00:00 CET

Komu



Phishingator noreply@phishingator.cesnet.cz

Martin.Sebela@cesnet.cz

Automatická notifikace systému Phishingator

Dne 18. 1. 2023 (21:45) Vám byl odeslán e-mail "Kalendář plánu mezd 2023 je nyní k dispozici (důležitý)". Jednalo se o cvičný phishing (podvodnou zprávu) s typickými znaky, které útočníci používají při snaze získat Vaše heslo, osobní údaje nebo číslo platební karty.

Gratulujeme, v testu jste obstáli :)

E-mail včetně indicií pro jeho rozpoznání si můžete prohlédnout zde:
<https://phishingator.cesnet.cz/phishing/5615479>

Děkujeme, že máte zájem vzdělávat se v oblasti phishingu.

Váš zbývající počet cvičných phishingových zpráv: 9
Změnu můžete provést po přihlášení na:
<https://phishingator.cesnet.cz>

Z pohledu uživatele



- **Přístupné všem** uživatelům organizace
- **Historie** přijatých e-mailů
 - **Reakce uživatele** na e-maily
 - **Indicie** k rozpoznání phishingu
- Možnost se dobrovolně přihlásit k **odebírání cvičného phishingu**
 - Nastavení limitu

Phishingator v1.2

Martin.Sebela **uživatel** [→ Odhlásit]

Moje účast v programu

[Nápověda](#)

Pro dobrovolné odebírání cvičného phishingu z Phishingatoru nebo naopak pro jeho zrušení stačí upravit volby v této sekci.

- 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, ale upozorní mě na hrozbu phishingu a na aktuální triky útočníků.
- 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](#)

© Martin Šebela, 2019–2023

Z pohledu administrátora – výsledky kampaně



- Zaznamenány reakce příjemců:
 - Bez reakce
 - Návštěva podvodné stránky
 - Vyplnění neplatných přihlašovacích údajů
 - Vyplnění platných přihlašovacích údajů
- Sledování průběžných výsledků
- Data zadaná na podvodné stránce (anonymizováno)

Systém pro rozesílání cvičných phishingových zpráv

Martin.Sebela (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).

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	10. 3. 2021	msebela	Spear phishing na mzdy	Přihlášení do SSO (věrná kopie)	http://login.████████.cz	173/173	každý den od 11:30	10. 3. 2021	11. 3. 2021	-

Konečné akce uživatelů v kampani

Akce	Count	Percentage
bez reakce	118	68.2 %
návštěva stránky	24	13.9 %
zadání neplatných údajů	9	5.2 %
zadání platných údajů	22	12.7 %

Tabulka konečných akcí

Konečné akce v kampani dle skupiny

Legend: bez reakce (green), návštěva stránky (blue), zadání neplatných údajů (yellow), zadání platných údajů (red)

Provedené akce v kampani

Akce	Count	Percentage
bez reakce	118	68.2 %
návštěva stránky	90	33.7 %
zadání neplatných údajů	37	13.9 %
zadání platných údajů	22	8.2 %

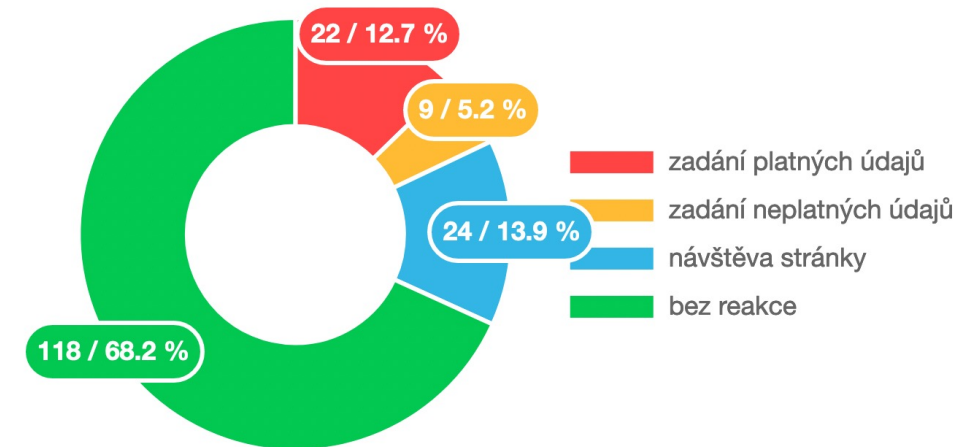
Tabulka všech provedených akcí

Příklad: Cvičný phishing na mzdy



- **Rozesláno 173** vybraným **zaměstnancům**
 - Napříč fakultami a dalšími odděleními
 - 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)**

Konečné akce uživatelů v kampani

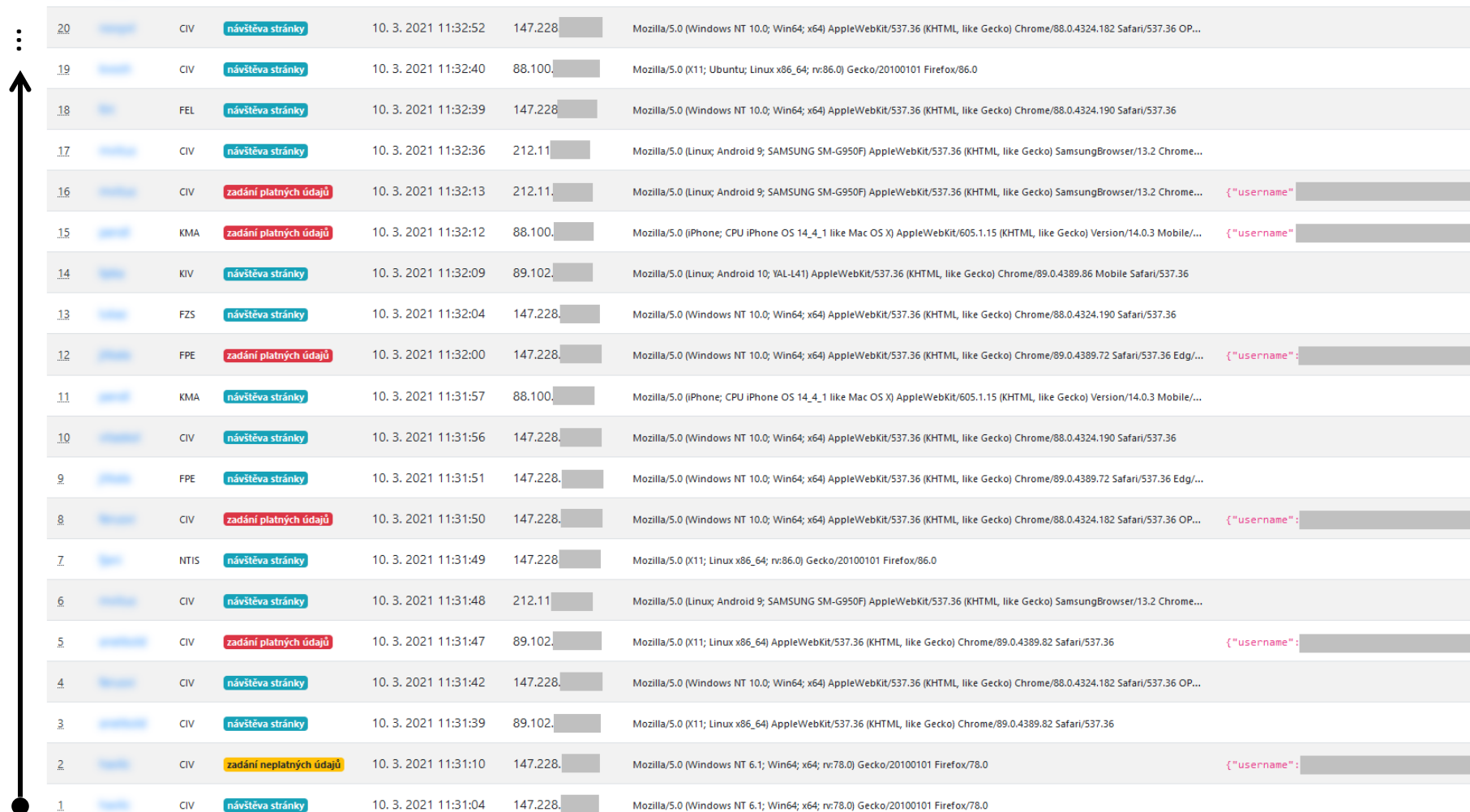


Příklad: Časová osa phishingové kampaně



- **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



A vertical timeline on the left side of the table, with an upward-pointing arrow, indicates the sequence of events corresponding to the list on the left. The table itself is a log of events, with rows numbered 1 to 20 from bottom to top. Each row contains a number, a status icon, a user agent, an event type, a timestamp, an IP address, and a browser user agent string. Some rows have a red box with the text '{ "username": ' followed by a greyed-out area.

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

Reakce příjemců



- Vyplnění **platných** přihlašovacích údajů

```
{"username":"nic ti nedam! a zdravim bezpecaky","..."}
```

- Vyplnění **neplatných** přihlašovacích údajů

- Překlepy
- **Vzkazy** od příjemců cvičného phishingu

```
{"username":"Sebe!a","password":"m..."}
```

⋮	101	...	návštěva stránky	10. 3. 2021 13:01:11	188.94. ...	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
↑	100	...	návštěva stránky	10. 3. 2021 12:59:09	147.228. ...	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935F) AppleWebKit/537.36 (KHTML, like Geck...
	99	...	zadání neplatných údajů	10. 3. 2021 12:58:32	147.228. ...	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935F) AppleWebKit/537.36 (KHTML, like Geck... {"username":"Děkuji za nabídku, aL...
⋮	98	...	návštěva stránky	10. 3. 2021 12:57:49	147.228. ...	Mozilla/5.0 (Linux; Android 8.0.0; SM-G935F) AppleWebKit/537.36 (KHTML, like Geck...

```
{"username":"Děkuji za nabídku, ale můj plat je více než adekvátní..."}
```

- **Hlášení** cvičného phishingu na helpdesk, IT oddělení
- **Debaty** o phishingu v kuloárech, u oběda, ...



- **Phishingator = nová služba CESNETu v oblasti bezpečnosti**
 - Nenásilná forma **vzdělávání uživatelů**
 - Cílem zvýšit povědomí o phishingu
 - Živý **vývoj**
- Poskytováno formou **Software as a Service**
 - Servery CESNETu, oddělená data i instance
 - Připravíme 3 podvodné stránky, 3 vzorové podvodné zprávy
 - Zaškolení administrátorů, L2 support
- **Zájem o Phishingator – Oddělení péče o uživatele**
 - Cenová nabídka, obchodní podmínky
 - *phishingator@cesnet.cz*

Dotazy



Martin Šebela

`martin.sebela@cesnet.cz`

CESNET FLAB