

BOIT

VYHODNOCENÍ TESTŮ

SOCIÁLNÍHO INŽENÝRSTVÍ

společnost: **Nemocnice Vitalice a.s.**



ÚVOD

Phishingový test je praktické cvičení určené k podpoře a měření účinnosti nastavených opatření a směrnic a ke zvyšování povědomí o kybernetické bezpečnosti pro koncové uživatele a managementu. Výsledky tohoto testu ukazují náchylnost pracovníků k útokům pomocí phishingu, ve kterých protivník obelstí uživatele e-mailu, aby klikl na škodlivý odkaz a získal neoprávněný přístup k síti.

ZODPOVĚDNÉ OSOBY

ZÁKAZNÍK

Nemocnice Vitalice

IČ: 361573261

E-mail: nemocnice@vitalice.cz

TESTER

Pavel Matějčíček

BOIT Cyber Security s.r.o.

E-mail: pavel.matejcek@boit.cz

CÍLE

- Provéřit odolnost lidského faktoru
- Zlepšit povědomí zaměstnanců o IT bezpečnosti
- Odhalit slabá místa v zabezpečení
- Ověřit účinnost nastavení e-mailových služeb a detekčních mechanismů

INTERNÍ IT

Jan Novák

Správce IT

E-mail: admin@vitalice.cz



01

Výsledky phishingového testu

Celkem **537** odeslaných e-mailů

51 %

Uživatelů otevřelo
podvodný e-mail a cíleně
načetlo jeho grafiku.

47 %

Uživatelů přešlo z
e-mailu cíleně na
podvodné stránky.

36 %

Uživatelů zadalo
přihlašovací údaje do
falešného formuláře.

Přihlášeno
193

E-mail otevřen
274

Kliknuto na odkaz
252

537

02

Popis kampaní

V rámci phishingového testu jsme realizovali tři tematické kampaně. Jednalo se o sociální inženýrství, které útočníci používají jak k hromadným kampaním, tak k takzvanému spear phishingu.

Ve Vašem případě byly použity tři kampaně, které cílily především na firemní stránku zaměstnanců.

Konkrétně se jednalo o témata:

- **Sken PDF z tiskárny**
- **Dochází místo ve sdílené složce**
- **Nové firemní benefity**

Cílem bylo dostat uživatele na podvodné stránky, které simulovaly firemní login do web mailu, který je dostupný z intranetu, ale má i svou on-line alternativu:

<https://vitalice.cz/owa>

Po prokliku se uživatel dostal na falešné stránky, kde jsme ho na phishing nijak neupozorňovali. Na podvodné stránce se pak uživatel měl možnost přihlásit a následně byl přesměrován na pravý web firemního webmailu.

Kampaň "**Nové firemní benefity**" splnila svůj účel a byla nejúspěšnější, uživatelé zadali přihlašovací údaje k firemním systémům do podvodných stránek.

Celkem **95 uživatelů e-mailů otevřelo**, **63 z celkového počtu přešlo i na podvodné stránky**.

Největší problém je pak počet uživatelů, kteří se na falešných stránkách přihlásili - tedy odevzdali firemní přihlašovací údaje útočníkům.

Jednalo se celkem o celých 36 % zaměstnanců, tedy **95 unikátních uživatelů kteří by tak společnost mohli kompromitovat**.

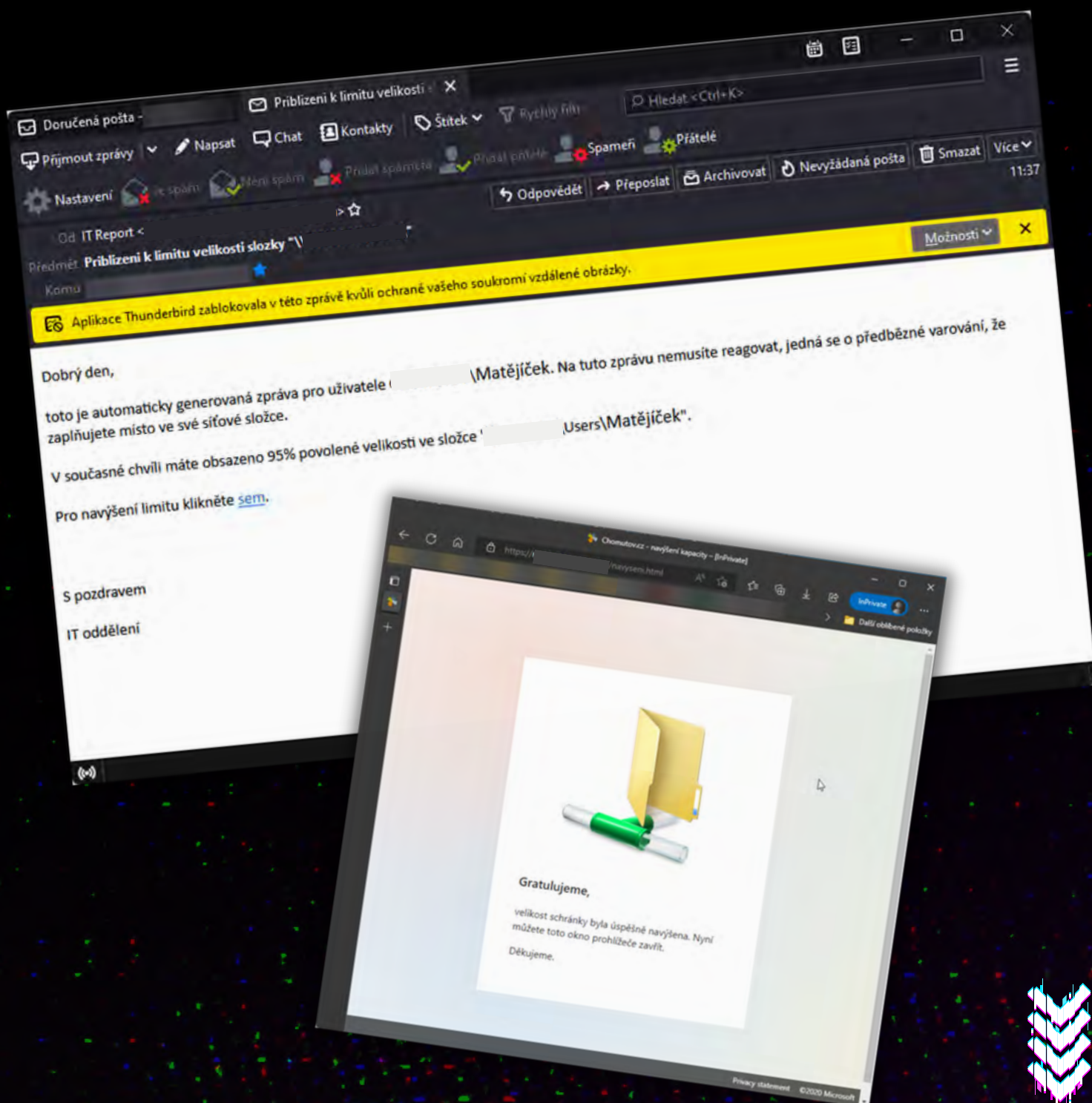
Pokud vztáhneme počet přihlášení k e-mailům o kterých víme že je uživatel prokazatelně otevřel, jedná se o celých **66 % zaměstnanců**.



Dochází místo na fileserveru

03

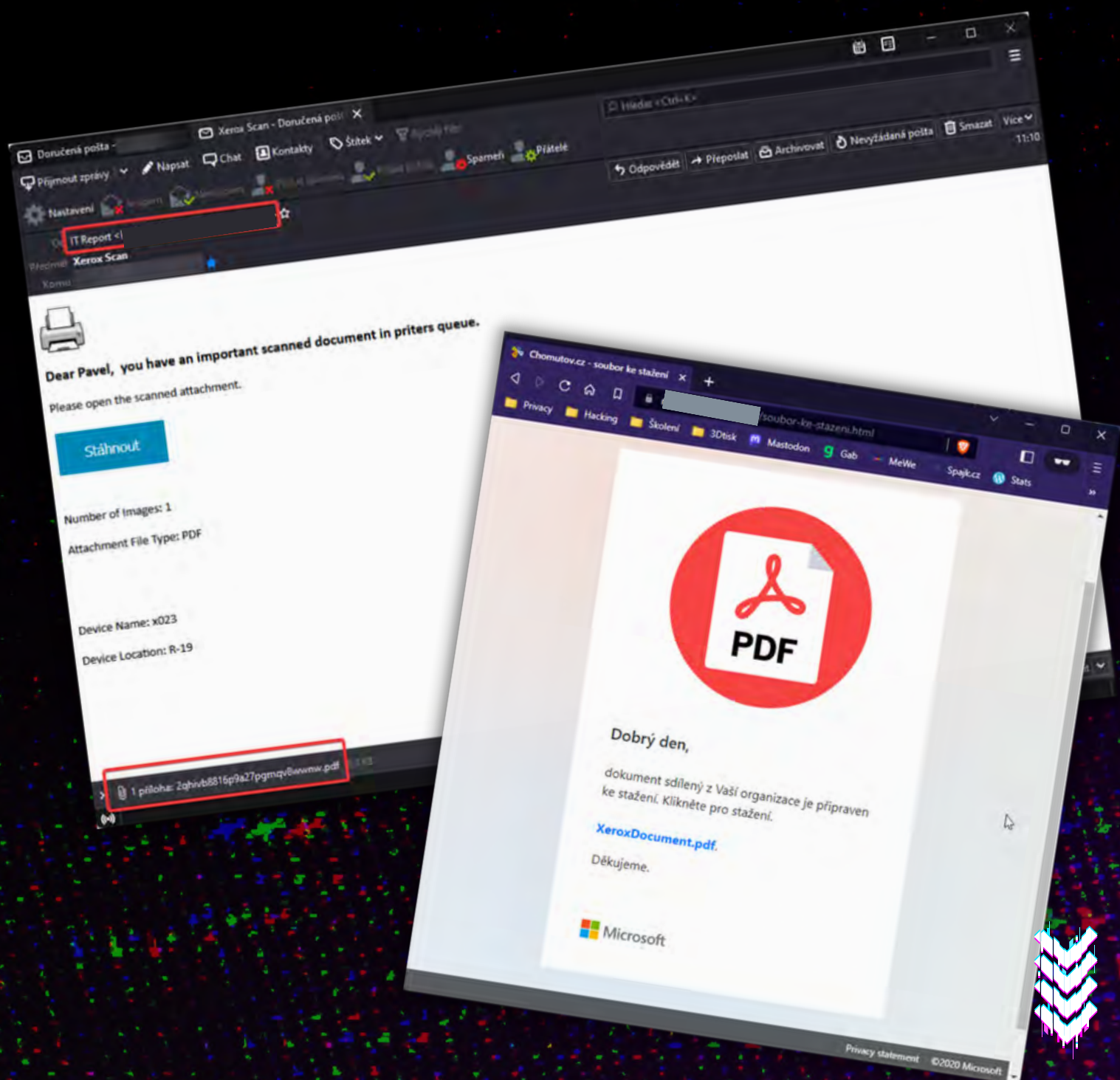
Tuto kampaň jsme poslali jako první na 132 zaměstnanců. 57 jich e-mail otevřelo, 48 se prokliklo na podvodnou stránku.



PDF scan z tiskárny

04

Tuto kampaň jsme poslali na 140 zaměstnanců, 74 jich e-mail otevřelo a 72 přešlo na podvodnou stránku. Zde mohli soubor stáhnout, učinilo tak minimálně 8 zaměstnanců.



Nové benefity

05

O dva dny později jsme poslali kampaň na všechny zaměstnance - 265 e-mailů. 145 zaměstnanců e-mail otevřelo (načetlo jeho grafiku), 134 se prokliklo na podvodnou stránku, 95 zadalo své přihlašovací údaje.



**Nemocnice
Vitalice +**

KRAJSKÁ NEMOCNICE A.S.

Nové benefity

Krásný den,

Jak jistě víte, od nového roku jsme spustili nový systém benefitů pro interní zaměstnance. S přicházejícím podzimem jsme přidali nové benefity, jejichž cílem je především Vaše zdraví - masáže, slevu do solné jeskyně i poukázky na vitamíny a čaje.

Portál pro obsluhu se nachází zde: <https://benefity.██████████.cz>

Pro přihlášení použijte stejné přihlašovací údaje, které používáte pro přihlášení do e-mailu či dalších systémů.

V případě jakýchkoliv dotazů nás neváhejte kdykoliv kontaktovat.

Stanislava ██████████

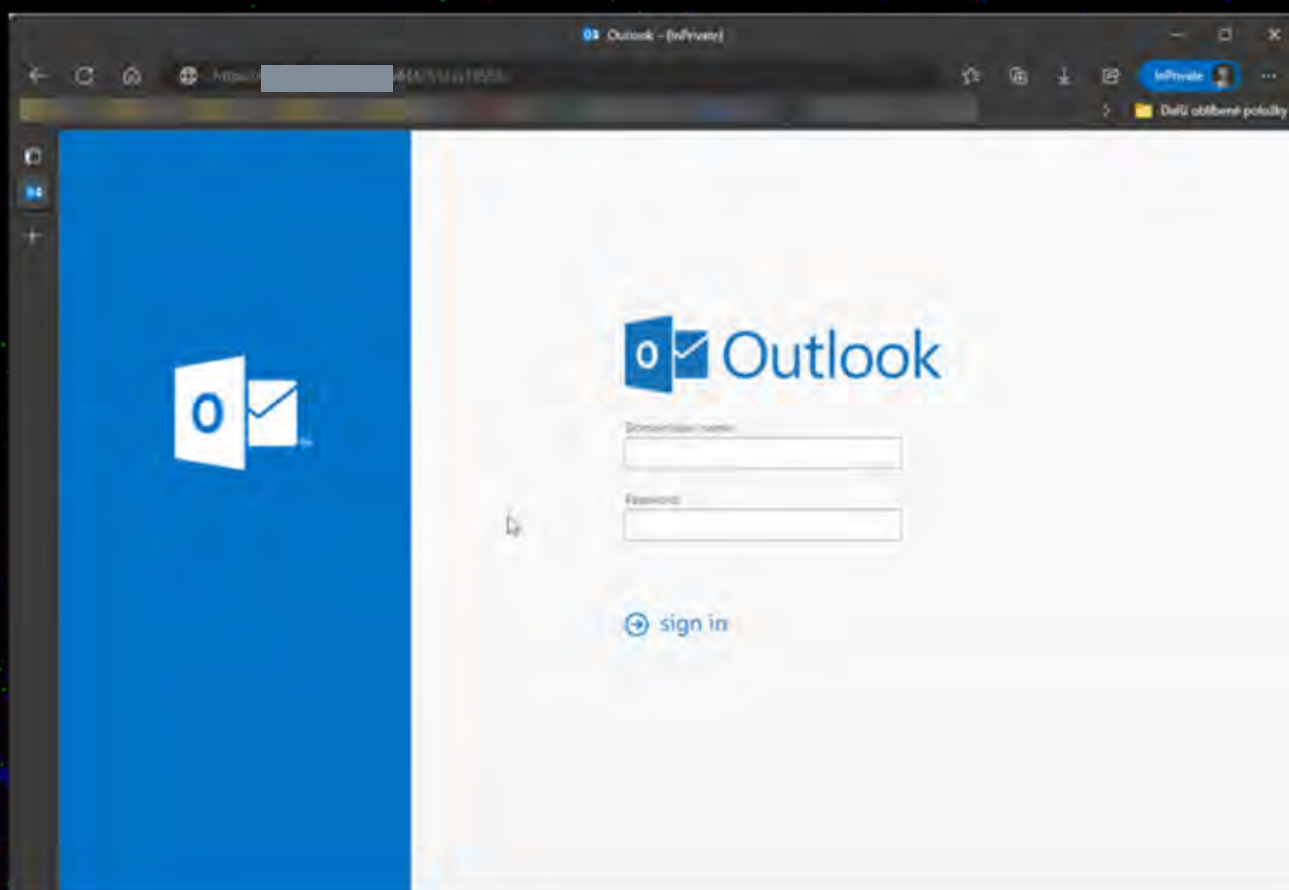
personalistka



Podvodná stránka

06

Zde je náhled podvodné stránky, na kterou byli zaměstnanci přesměrováni. Po navštívení stránky mohou útočníci zjistit IP adresu, typ a verze operačního systému a verze a typ webového prohlížeče každého zaměstnance. Na tyto stránky přešlo celkem 47 % obeslaných uživatelů (celkem), 95 zaměstnanců se pak přihlásilo. Stránka běžela na webu **nemocnice-vitalice.cz**.



07

Výsledky vishingového testu

Celkem **50** telefonních hovorů

90 %



Uživatelů přijalo hovor z
neznámého čísla.

40 %

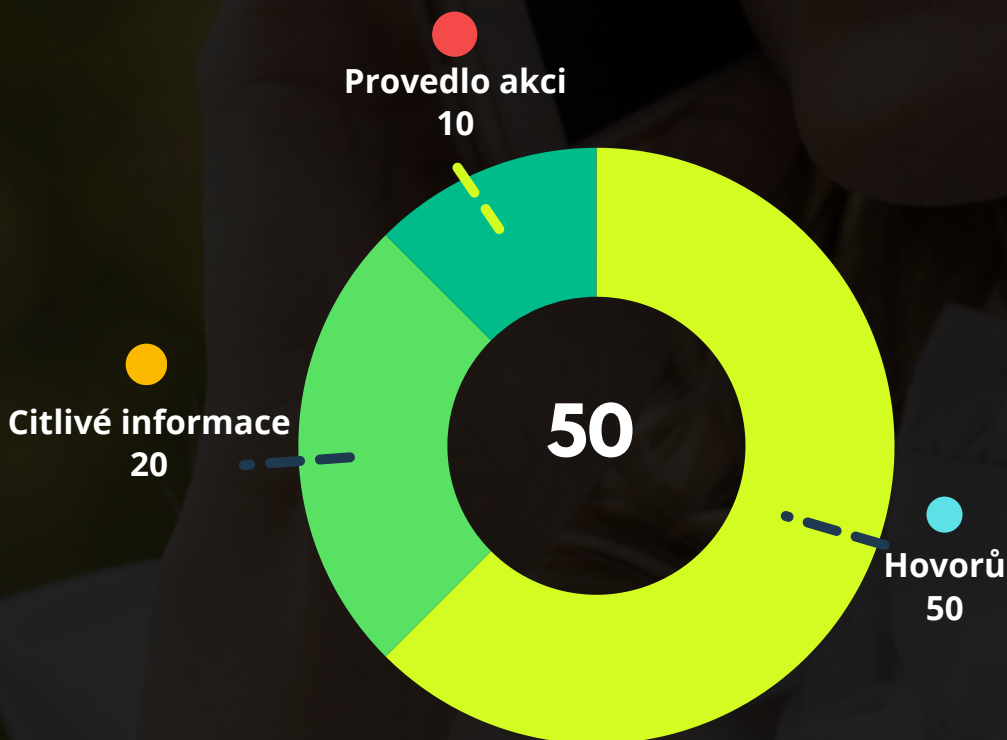


Uživatelů vyzradilo
informace citlivého
charakteru.

20 %



Uživatelů vykonalo
akci, kterou po nich
volající požadoval.





Popis vishingových kampaní

V rámci vishingového testu jsme cílili na dvě měřitelné hodnoty - vyzrazení citlivých informací a vykonání akce požadované útočníkem.

Za citlivé informace považujeme:

- ověření osobních údajů/potvrzení totožnosti dotyčného
- získání e-mailové adresy na dalšího zaměstnance, neuvedeného v kontaktních informacích společnosti
- údaje o použitých technologiích (VPN, antivirus) či možnostech vzdáleného připojení

Vykonané akce:

- přechod na podvodnou stránku a kliknutí na odkaz
- zadání uživatelského jména a hesla
- stažení programu
- otevření přílohy z e-mailu

Ve vaší společnosti jsme z 50 hovorů docílili 45 zvednutí, 5 uživatelů na hovor z neznámého čísla nereagovalo.

10 zaměstnanců nám prozradilo, jaký typ VPN používáte a jaký máte antivirový program.

10 dalších uživatelů nám pak prozradilo kontakt na pracovníky fakturačního oddělení, který se nenachází na webu společnosti.

5 zaměstnanců přešlo na podvodnou stránku, kde jsme logovali jejich IP a adresu a věděli jsme tak, za se nacházejí na pracovišti nebo na home-office.

Dalších 5 uživatelů pak ze stránek stáhlo podvodný soubor a otevřelo jej.





Výsledky baitingového testu

Celkem **10** nastražených USB

60 % 

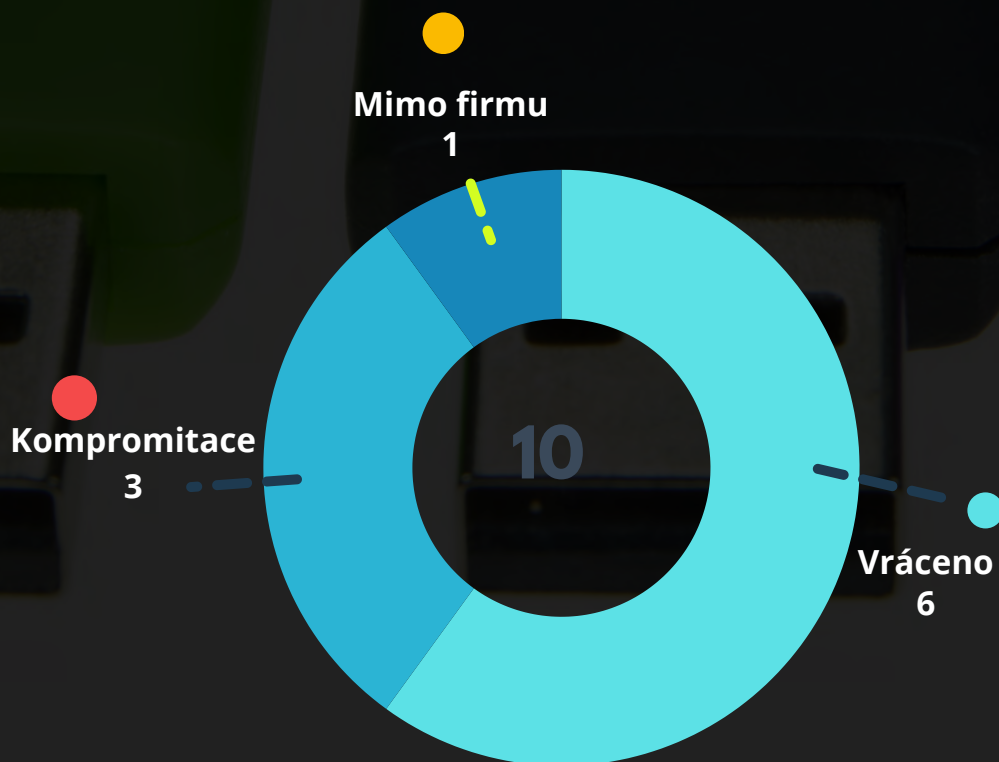
USB se vrátilo
administrátorovi,
uživatelé nález nahlásili.

30 % 

USB bylo použito na
firemních zařízeních
a došlo k otevření
souboru.

10 % 

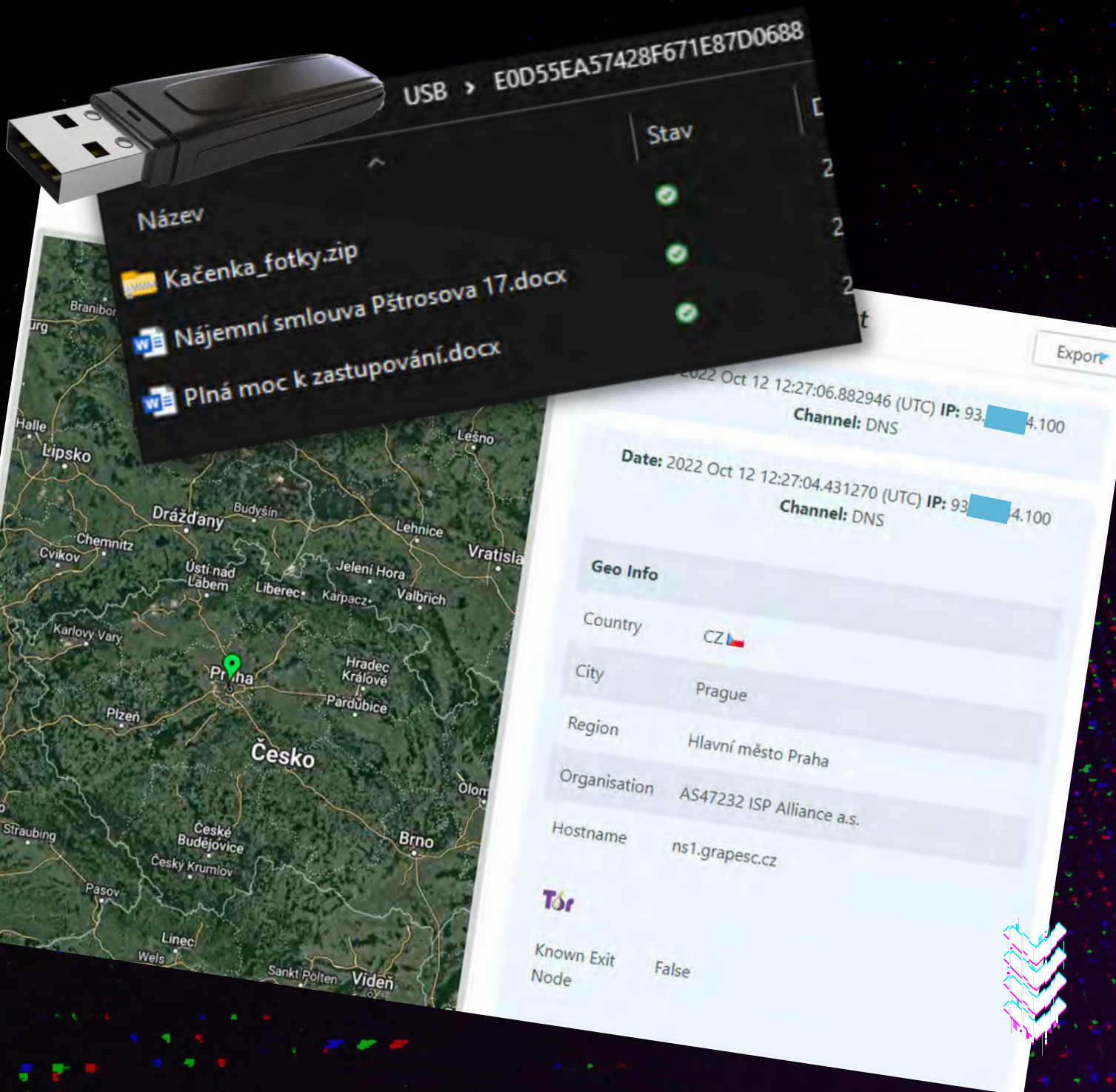
USB se ztratilo,
následně došlo k
otevření z lokality
mimo pracoviště.



USB baiting

10

Je forma sociálního inženýrství, která cílí na zvědavost uživatelů. Na USB discích, které jsme nastražili v prostorách společnosti, jsou připraveny dokumenty s citlivými údaji. Po otevření dokumentu můžeme zjistit IP adresu, ze které k otevření došlo, útočníci by však dokázali nastraženým malwarem společnost kompromitovat.



SEZNAM DOPORUČENÍ

1.) Informujte zaměstnance a nezainteresovaný management o tom, že proběhly testy sociálního inženýrství a sdělte jim výsledky. Ideální forma je krátký e-mail.

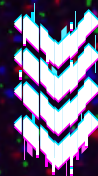
2.) Realizujte školení IT bezpečnosti, kde budou všichni zaměstnanci poučeni o problematice phishingu a sociálního inženýrství. Doporučujeme neprovádět jej svépomocí, ale pomocí externisty, neboť zaměstnanci vnímají člověka „z venku“ jako autoritu.

3.) Zvažte update již nepodporovaných systémů Windows 7 a Windows 8, které byly zjištěny, případně jejich izolování ve speciálním segmentu sítě.

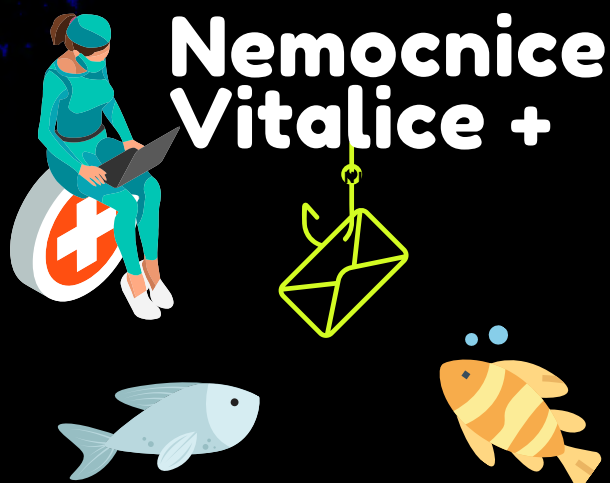
4.) Po čase, ideálně 3-6 měsících, doporučujeme testy zopakovat, s jinými scénáři a na jiná témata.



5.) Nezapomeňte deaktivovat nastavené výjimky v antiSPAM a antivirových modulech. V případě realizace dalších testů je nemažte, bude stačit je aktivovat.



VÝSLEDEK



v testu jste neuspěli

Útočníci by společnost dokázali snadno kompromitovat.

Tak by se dal shrnout výsledek, kdy **95 zaměstnanců naletělo** na podvodné e-maily a odevzdali přihlašovací údaje do systémů společnosti útočníkům, **3 další zapojili nalezená USB** do firemních zařízení a **10 dalších** podlehl útočníkům po telefonu.

Výsledek je to horší než je běžné, median se pohybuje kolem 20 procent.

Pokud by se jednalo o reálný útok, mohlo by dojít k narušení bezpečnosti, omezení provozuschopnosti společnosti, finančním ztrátám a negativní publicitě.

