Phishingový útok prakticky

Radek Janoštík

Univerzita Palackého v Olomouci

15. 2. 2024

Outline

- Úvod
- Email a jeho podvržení
- Získání přihlašovací stránky
- Samotné provedení
- Jak se bránit
- Závěr

Podmínky zápočtu

- Účast na cvičení není povinná
- Z každého cvičení bude úkol

Podmínky zápočtu

- Účast na cvičení není povinná
- Z každého cvičení bude úkol
- Deadline odevzdání: Následující cvičení
- Možné ukázat osobně či emailem (video?)

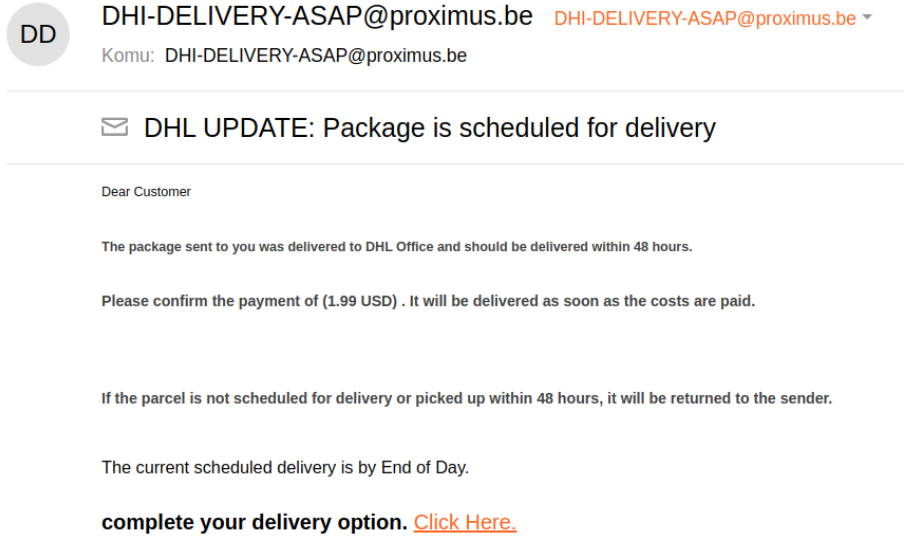
Podmínky zápočtu

- Účast na cvičení není povinná
- Z každého cvičení bude úkol
- Deadline odevzdání: Následující cvičení
- Možné ukázat osobně či emailem (video?)
- Je potřeba splnit 80 % úkolů
- Dva úkoly je možné odevzdat „opožděně“ do konce zápočtového týdne (pátek 10.5.2024)

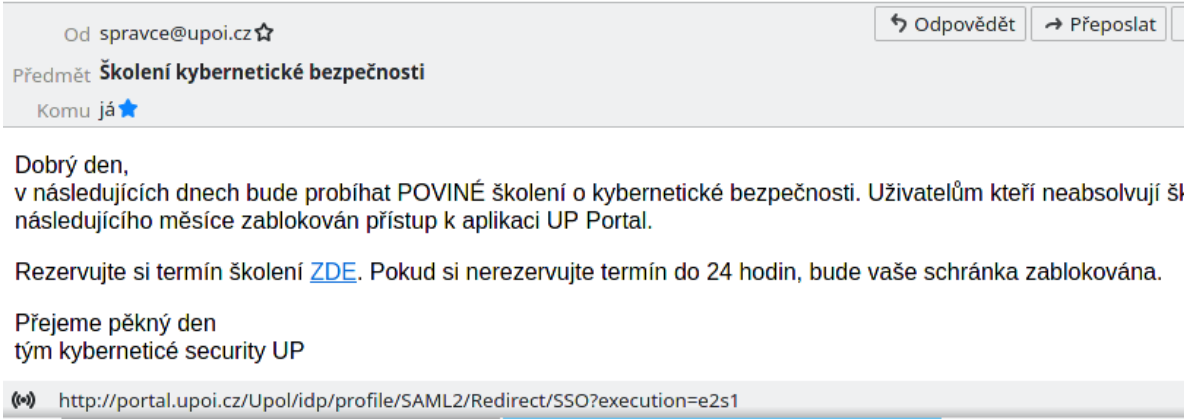
Co je to phishing

- Podvodný způsob, jak získat uživatelovy důvěrné údaje (přihlašovací, číslo karty, . . .)
- Technická a sociálně-inženýrská část
- $\Rightarrow$ Vyvolání uživatelovy důvěry
- Často spojen s podvržením emailu
- Historie (Ezau a Jákob, můj první phishingový útok, covid)

Ukázka


DD
DHI-DELIVERY-ASAP@proximus.be
DHI-DELIVERY-ASAP@proximus.be
Komu: DHI-DELIVERY-ASAP@proximus.be
DHL UPDATE: Package is scheduled for delivery
Dear Customer
The package sent to you was delivered to DHL Office and should be delivered within 48 hours.
Please confirm the payment of (1.99 USD) . It will be delivered as soon as the costs are paid.
If the parcel is not scheduled for delivery or picked up within 48 hours, it will be returned to the sender.
The current scheduled delivery is by End of Day.
complete your delivery option. Click Here.

Ukázka


Od spravce@upoi.cz
Odpovědět
Přeposlat
Předmět Školení kybernetické bezpečnosti
Komu já
Dobrý den,
v následujících dnech bude probíhat POVINÉ školení o kybernetické bezpečnosti. Uživatelům kteří neabsolvují šk
následujícího měsíce zablokován přístup k aplikaci UP Portal.
Rezervujte si termín školení ZDE. Pokud si nerezervujte termín do 24 hodin, bude vaše schránka zablokována.
Přejeme pěkný den
tým kybernetické security UP
http://portal.upoi.cz/Upol/idp/profile/SAML2/Redirect/SSO?execution=e2s1

Anketa

- Kdo už někdy zažil (a odhalil)?

Anketa

- Kdo už někdy zažil (a odhalil)?
- Kdo už někdy naletěl (a uvědomil si to, ale pozdě)?

Anketa

- Kdo už někdy zažil (a odhalil)?
- Kdo už někdy naletěl (a uvědomil si to, ale pozdě)?
- Kdo už někdy naletěl a uvědomil si to až po následcích?

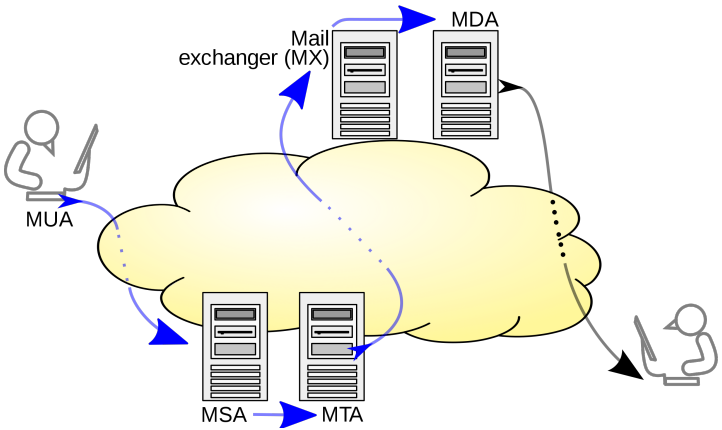
Anketa

- Kdo už někdy zažil (a odhalil)?
- Kdo už někdy naletěl (a uvědomil si to, ale pozdě)?
- Kdo už někdy naletěl a uvědomil si to až po následcích?
- Kdo už někdy zkoušel provést?

SMTP – Protokol pro email v kostce

- Velmi starý protokol ($\approx$ 1982)
- Navržen bez důrazu na bezpečnost
  - Bez autentizace uživatelů
  - Bez šifrování
  - Pouze textová komunikace
- Uživatel má „svůj“ server pro odesílání pošty
- Server podle adresy zjistí, kam má email přeposlat
- Email doputuje do cílové schránky
- Jednotlivé uzly si (většinou) důvěřují
- Součástí zprávy jsou *hlavičky* nesoucí servisní informace, opět slepá důvěra

SMTP v obrázku



Obrázek: zdroj:
`https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol#/media/File:SMTP-transfer-model.svg`

Podvržení emailu

- Máme-li přístup k nějakému serveru pro odchozí poštu, můžeme zmanipulovat hlavičky
- Hlavičkám (většina) klienti *věří* a moc je nekontrolují
- V hlavičkách můžeme například nastavit odesílatele jiného než jsme my
- Lze změnit i datum odeslání
- Ukázka (hlavičky, podrvržení odesílatele, data)

Simulace přihlašovací stránky

- Většina dnešních phishigových útoků simuluje reálnou přihlašovací stránku
- Není problém ukradnout jakoukoliv stránku
- $\Rightarrow$ Cokoliv je zobrazitelné v prohlížeči, jde snadno ukradnout
- Občas to chce trochu snahy a vůle (vše je otázkou peněz)
- Pojďme ukradnout univerzitní přihlašovací stránku
  - Zjistíme *kde* stránka vlastně je
  - Stáhneme si ji
  - A mírně upravíme
  - Ukázka

Provedení

- Přihlašovací stránku umíme ukradnout
  - Zbývá ji vyvěsit někam na internet a „oživit“

Provedení

- Přihlašovací stránku umíme ukradnout
  - Zbývá ji vyvěsit někam na internet a „oživit“
- Umíme odeslat falešný email, je třeba zjistit „živé“ emailové adresy
  - Na internetu se válí velké množství uniklých dat – např. Facebookleak 2019
  - Na univerzitě by mohlo jít generovat (příjmení, jméno, číslo)
  - Někde koupit
  - ...

Provedení

- Přihlašovací stránku umíme ukradnout
  - Zbývá ji vyvěsit někam na internet a „oživit“
- Umíme odeslat falešný email, je třeba zjistit „živé“ emailové adresy
  - Na internetu se válí velké množství uniklých dat – např. Facebookleak 2019
  - Na univerzitě by mohlo jít generovat (příjmení, jméno, číslo)
  - Někde koupit
  - ...
- Teď už jen zbývá vytvořit nějakou důvěryhodnou zprávu a jít „rybařit“

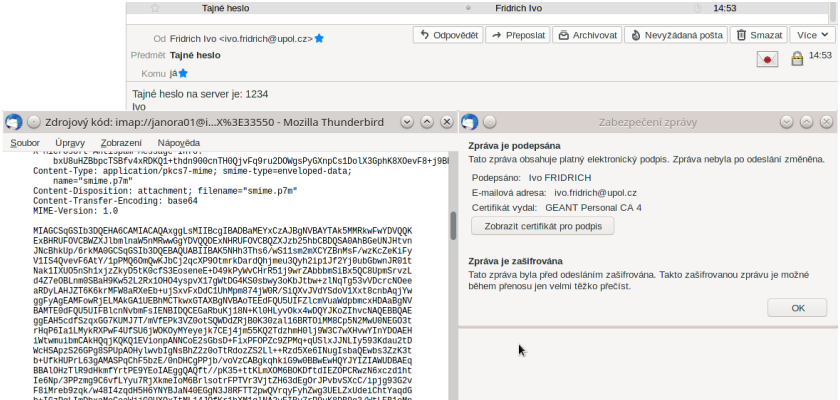
Provedení

- Přihlašovací stránku umíme ukradnout
  - Zbývá ji vyvěsit někam na internet a „oživit“
- Umíme odeslat falešný email, je třeba zjistit „živé“ emailové adresy
  - Na internetu se válí velké množství uniklých dat – např. Facebookleak 2019
  - Na univerzitě by mohlo jít generovat (příjmení, jméno, číslo)
  - Někde koupit
  - ...
- Teď už jen zbývá vytvořit nějakou důvěryhodnou zprávu a jít „rybařit“
- Ukázka

Jak se bránit

- Útok na uživatelovu neznalost ⇒ osvěta
  - Všímat si detailních nesrovnalostí
  - Špatný pravopis, chybějící diakritika
  - Neklikat slepě na odkazy, všímat si jejich URL adresy
  - Nikomu neposílat hesla
  - Slepě neotevírat přílohy
  - „Zelený zámeček“ neznamená pravá stránka
- Technická omezení – SMTP servery by neměly fungovat bez ověření
- Digitálně podepisovat zprávy + případné šifrování
  - Cesnet poskytuje osobní certifikáty zdarma
    `https://pki.cesnet.cz/cs/ch-tcs-p-crt-crl.html`
  - Nařízení používat (př. TU Dresden)
- Dvoufaktorové ověření (mnohem těžší na útok)

Ukázka šifrování a podpisu



Obrázek: Šifrovaný a podepsaný email

Závěr

- Jak vidíte, udělat jednoduchý útok není složité

Závěr

- Jak vidíte, udělat jednoduchý útok není složité
- Co vše by šlo lépe nasimulovat s finanční motivací

Závěr

- Jak vidíte, udělat jednoduchý útok není složité
- Co vše by šlo lépe nasimulovat s finanční motivací
- Co si odnést? Buďte obezřetní, všímejte si detailů, kontrolujte URL

Úkol

- Veberte si nějakou webovou stránku a zkuste nasimulovat provedení útoku
  - „Ukrást a oživit“ přihlašovací stránku
  - Vytvořit smysluplný, uvěřitelný email
  - Pošlete mi jej se zmanipulovanými hlavičkami