

## **ODBOR POČÍTAČOVEJ KRIMINALITY**

ÚRADU KRIMINÁLNEJ POLÍCIE

PREZÍDIA POLICAJNÉHO ZBORU

### **Aktuálne trendy foriem počítačovej kriminality**



**kpt. Mgr. Marek Švarc**  
**mjr. JUDr. Zoltán Štiavnicky**

### **Vybrané druhy počítačových útokov**

- Phishing
- Pharming
- Sniffing
- Cracking
- Skimming
- Škodlivý kód

## **Phishing**

- obdržanie podvodnej e-mailovej správy,
- e-mailová správa obsahuje odkaz, ktorý nás presmeruje na podvodnú stránku, alebo na stránku kde sa náš počítač infikuje škodlivým kódom,
- Podvodná stránka od nás požaduje rôzne údaje ako napríklad meno, priezvisko, číslo kreditnej karty, PIN kód kreditnej karty alebo jednotlivé pozície z GRID karty.

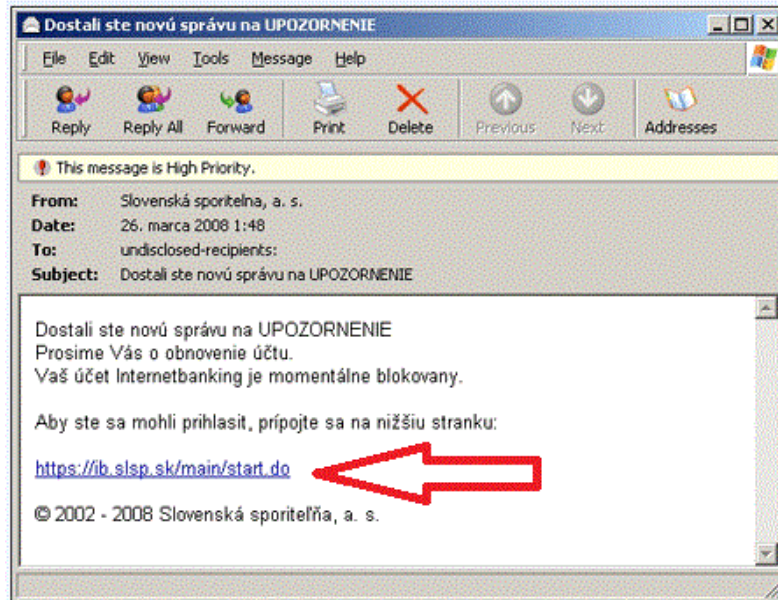


## **Pharming**

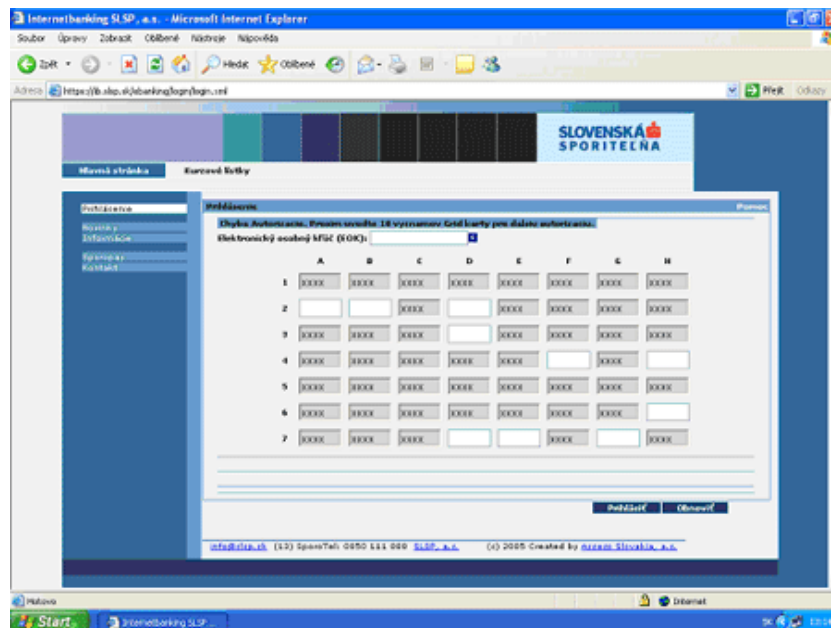
- založený na zmene DNS položiek (Domain Name System),
- užívateľ je presmerovaný na inú stránku,
- dizajn stránok je veľmi podobný ako pravá stránka spoločnosti,



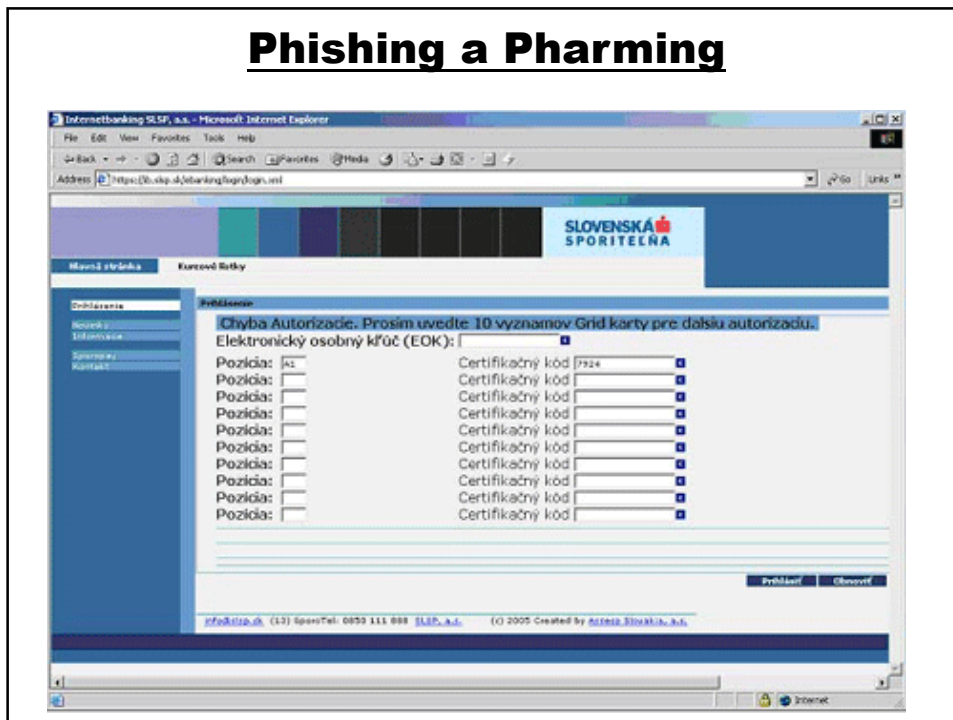
# Phishing



# Phishing a Pharming



## Phishing a Pharming



## Phishing a Pharming



## Pharming

- pharming založený na zmene „hosts“ súboru
- súbor „hosts“ slúži na nastavenie DNS záznamov



## Pharming

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name,
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10      x.acme.com              # x client host
127.0.0.1        localhost
```

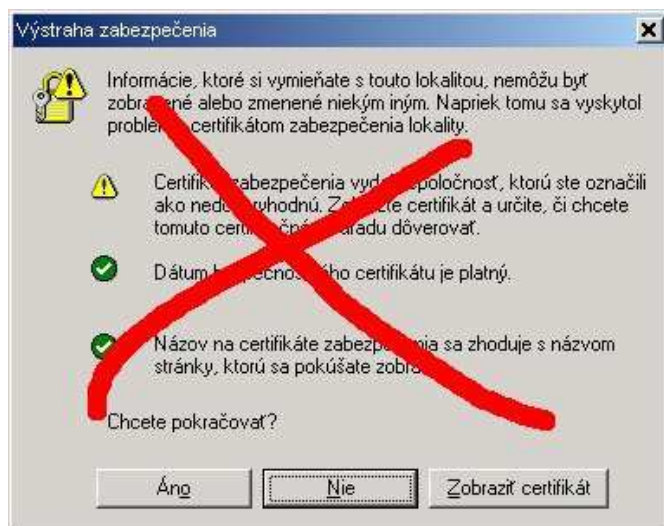
## Ako odhaliť phishing a pharming?

- pri phishingu je potrebné všímať si URL adresu webovej stránky na ktorej sa nachádzame,
- banka nikdy nevyžaduje od klientov citlivé osobné údaje či prístupové údaje do IB,
- chyby certifikátov zabezpečenia webových stránok.

## Ako odhaliť phishing a pharming?

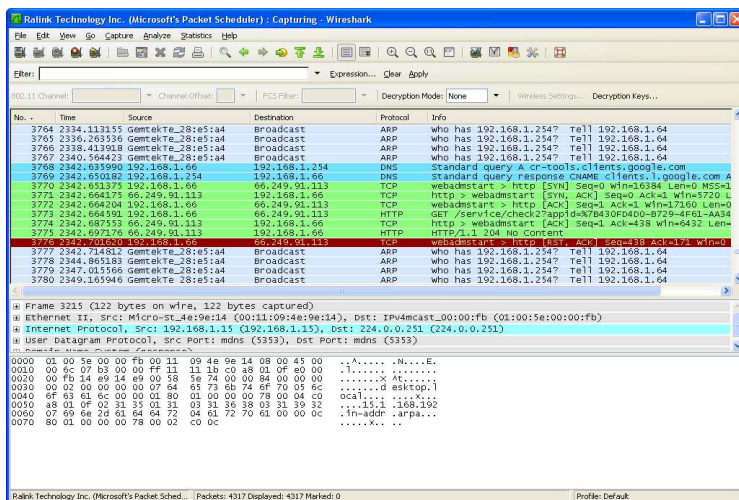
The screenshot shows a browser window with the address bar containing the URL [http://bradstem.com/bran/6\\_slp\\_01.html](http://bradstem.com/bran/6_slp_01.html), which is circled in red. The page content includes a login form with fields for 'Prístupové meno' and 'Prístupové heslo', and a 'Prísť kardi' button. Below the login form is a 'Vyber jazyk' section with radio buttons for 'Automicky/Default', 'Česky', 'English', and 'Slovenčina'. A news section titled 'Pozor na podobné e-maily (publikované 25.03.2008 13:32:39)' is visible. At the bottom, there is a warning banner: 'Pharming/Phishing "Pozor na útoky"' with a skull and crossbones icon.

## Ako odhaliť phishing a pharming?



## sniffing

- odchyťovanie komunikácie v počítačovej sieti osobou, ktorá nie je adresátom takejto komunikácie



## Opatrenia proti sniffing

- odhaliť sniffing pre bežného užívateľa je takmer nemožné,
- Nevyužívať voľne prístupné pripojenia k internetu na (freewifi, internetové kaviarne) .

## Cracking

- protiprávny zásah, skúmanie alebo úprava zdrojového kódu softvéru, umožňujúca prelomenie jeho ochrany.

The screenshot shows a debugger interface with three main panels:

- Registers (FPU):** Shows various registers such as EAX (00000000), ECX (0012FFFA), EDI (7C910738), and EIP (00401000).
- Disassembly:** Shows assembly instructions with addresses, hex, and mnemonics. For example:
 

```
00401000 75 05 00 PUSH 0
      00401001 58 1F0400 PUSH mkr_cn_3.00401000
      00401002 55 00 00 PUSH 0
      00401003 58 00 00 PUSH 0
      00401004 58 21000000 CALL <FPU.USER32.MessageBox>
      00401005 55 00 00 PUSH 0
      00401006 58 00000000 PUSH mkr_cn_3.00401000
      00401007 58 00000000 PUSH mkr_cn_3.00401000
      00401008 58 00000000 CALL <FPU.USER32.MessageBox>
      00401009 55 00 00 PUSH 0
      0040100A 58 01000000 CALL <FPU.LikeKernel32.ExitProcess>
      0040100B 55 00 00 PUSH 0
      0040100C 58 00204000 JMP DWORD PTR DS:[<kernel32.ExitProcess>]
      0040100D 58 00204000 JMP DWORD PTR DS:[<user32.MessageBox>]
```
- Memory:** Shows a memory dump for 'mkr\_cn\_3.<ModuleEntryPoint>' with addresses and hex values.



# Cracking



# Skimming



## Skimming



## Skimming



## Škodlivý kód

- škodlivý kód (*Malware, počítačový vírus, červ*) pochádza zo spojenia dvoch anglických slov *malicious* (škodlivý) a *software* (softvér). Ide o škodlivý softvér, ktorý má prevziať kontrolu nad počítačom obeť.



## Ransomware

- druh škodlivého kódu, ktorým zločinci vydierajú užívateľov aby im zaplatili buď sumy pre fiktívny dôvody alebo priamo výkupné za ich dáta,
- tvári sa ako výzva štátneho orgánu na zaplatenie pokuty za spáchaný trestný čin alebo priestupok (porušenie autorských práv, nedovolená distribúcia detskej pornografie, šírenie spamu, neoprávnený prístup k údajom atď.).

# Ransomware

**Pozor!**

**IP:** [REDACTED]

**Lokalita:** [REDACTED]

**Pozor! Váš počítač je zablokovaný kvôli aspoň jednému z dôvodov uvedených nižšie.**

Bol ste porušené "autorské práva a slobodných práv" (Videá, hudba, Software) a nedovolené použitie alebo distribúcia obsah chránený autorskými právami, a tým porušíte článok 128 trestného zákonníka Slovenskej republiky.

Článok 128 trestného zákonníka stanovuje pokutu 2 500 minimálnej mzdy alebo prostredníctvom slobody na 2 až 8 rokov.

Bol ste slyšení pri prezere alebo distribúciu zakázané produkcie pornografickým obsahom (Detská pornografia / Zoofília a atď.). A tým porušujete článok 202 trestného zákonníka Slovenskej republiky.

Článok 202 trestného zákonníka stanovuje odňatie slobody na 4 až 12 rokov.

Prostredníctvom prístup k počítačovým údajom bol zahájený z počítača, alebo ste boli ...

Článok 208 trestného zákonníka stanovuje pokutu až do výšky 100 000 € / alebo odňatie slobody po dobu 4 až 9 rokov.

Prístupové prístup bol zahájený z vášho počítača bez vášho vedomia alebo sohlasu, môže byť počítač infikovaný škodlivým softvérom, tak čo spôsobí záskok z používania Použitie osobného počítača.

Článok 210 trestného zákonníka stanovuje pokutu 2 000 libier na 50 000.

Spam distribúcia alebo iné protiprávne licencie bola uskutočnená z vášho počítača ako súhlasíte o zisk činnosti alebo bez vášho vedomia, môže váš počítač infikovaný škodlivým softvérom.

Článok 212 trestného zákonníka stanovuje pokutu až do výšky 250 000 € a zbavenie osobnej slobody až na 6 rokov. V prípade, že je táto činnosť bola uskutočnená bez vášho vedomia, tá sa uplatňuje do výšky uvedeného článku 210 trestného zákonníka Slovenskej republiky.

Všet osobnosť a adresa sú v súčasnej dobe určené kriminálny prípad sa začne proti vám v rámci jednoty alebo viacerých článkov uvedených vyššie, počas nasledujúcich 72 hodín.

Práda nového trestného zákona Slovenskej Republiky 28. augusta 2012, tento článok porušenie (ak sa neopíše - prvky) môže možno porušiť za podmienené prípad, že by ste zaplatiť pokutu štátu.

Pokuty môžu byť vyžaté až do pozas 72 hodín po porušení. Akonáhle 72 hodín uplynú, môžete zaplatiť pokutu opticky, a trestné konanie je zastavené prvý čas automaticky počas najbližších 72 hodín!

**Výška pokuty je SKK 2000 alebo €100. Môžete zaplatiť pokutu pomocou PaysafeCard alebo Ukash.**

Ked platíte pokutu, bude váš počítač si odmietať v 1 až 72 hodín od penize budú vložene do vášho účtu.

© -POLICAJNY ZBOR SLOVENSKEJ REPUBLIKY-

## Malware rôzneho druhu

- páchatelia často využívajú neopatrnosť a dôveru užívateľov,
- prostredníctvom e-mailových správ odosielaajú v prílohe (\*.pdf, \*.jpg, \*.zip) malware rôzneho druhu a následne získavajú kontrolu nad počítačom obete.

## **Sociálne inžinierstvo**

- je typ útoku využívajúci manipuláciu osôb za účelom vykonania určitej akcie (napríklad spustenia nejakého súboru) alebo získania určitých informácií. Sociálne inžinierstvo môže prebiehať osobne, prostredníctvom komunikačného prostriedku (telefón, mail, ..) alebo prostredníctvom úpravy prostredia (napríklad zanechanie média na dostupnom mieste). Obrana voči všetkým formám sociálneho inžinierstva je takmer nemožná.

## **Opatrenia proti sociálnemu inžinierstvu**

- V prípade, že ste kontaktovaný prostredníctvom mailu, alebo telefónu so žiadosťou o poskytnutie informácií dôverného charakteru (heslá, žiadosť o poslanie dokumentov, ...) aj zo strany zdanlivo dôveryhodného a oprávneného zdroja, je potrebné si dôveryhodnosť tohto zdroja overiť iným komunikačným kanálom (napríklad zavolať na známe číslo tejto dôveryhodnej osoby, ...),
- Organizácie by mali mať určené pravidlá, akým spôsobom sa môže žiadať o informácie z prostredia mimo organizácie a vytvoriť autentifikačné mechanizmy na overenie totožnosti,
- Neposkytujte dôverné informácie osobe, ktorej identitu si neviete overiť.

### **Nigerijske listy**

- je to druh podvodu, kedy sa útočník snaží vylákať od obete peniaze pomocou vymysleného (väčšinou dojemného) príbehu o zdedení peňazí, výhre, potrebe pomoci a pod.

### **Fakemail (falošný –email)**

- veľmi často využívaný spôsob ako oklamať obeť,
- dá sa zistiť len analýzou hlavičky e-mailovej správy.

## Fakemail (falošný –email)



Free online instant mailer with attachments, encryption,  
HTML editor and advanced settings...

✔ Fake mail sent successfully

**From Name:**

**From E-mail:**

**To:**

**Subject:**

**Attachment:**  Nie je zvolený súbor.

**Content-Type:**  text/plain  text/html  Editor

**Text:**

## kontakt



kpt. Mgr. Marek Švarc,  
[marek.svarc@minv.sk](mailto:marek.svarc@minv.sk),  
Klapka: 09610/50143  
Mobil: 0908/633184

mjr. JUDr. Zoltán Šťavnický,  
[zoltan.stavnicky@minv.sk](mailto:zoltan.stavnicky@minv.sk),  
Klapka: 09610/50172  
Mobil: 0917/648676

*Ďakujeme za pozornost!*

**OTÁZKY ?**

