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

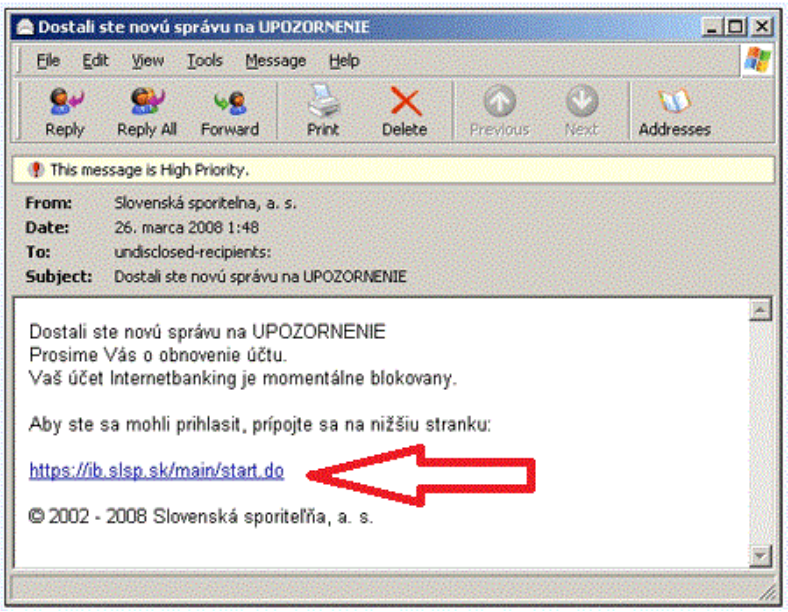
Phishing

- 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.

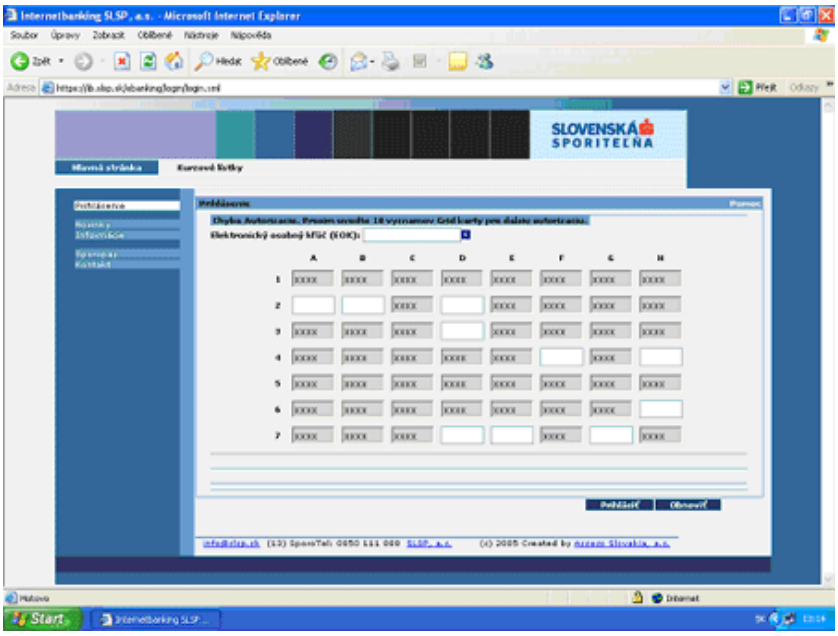
Pharming

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

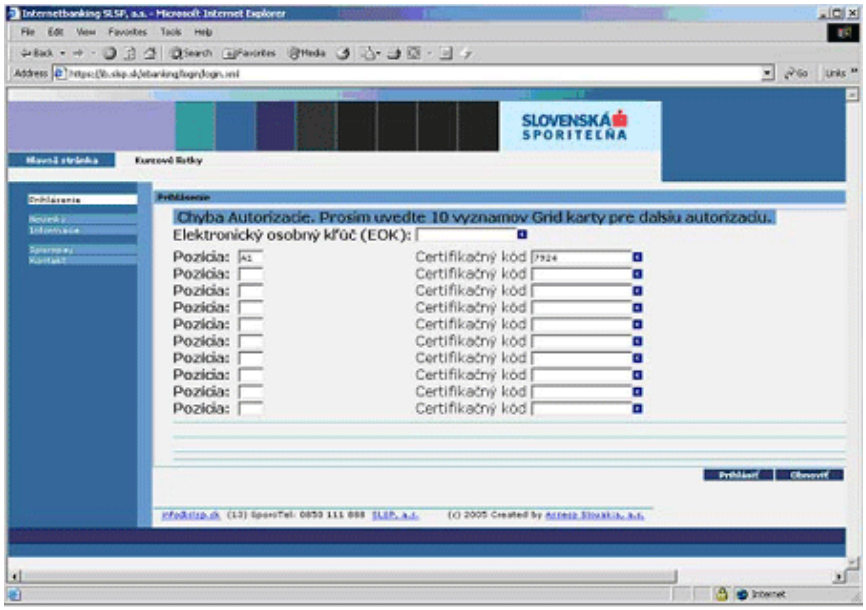
Phishing



Phishing a Pharming



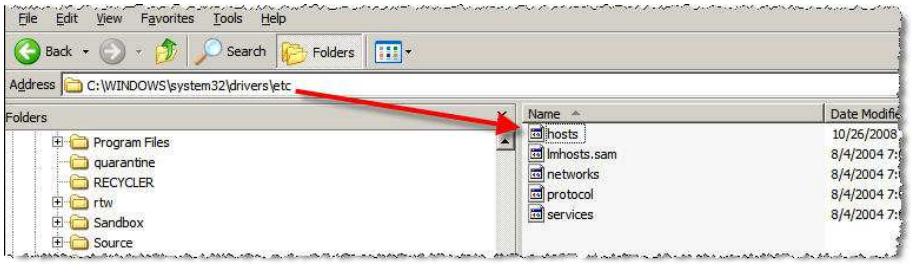
Phishing a Pharming



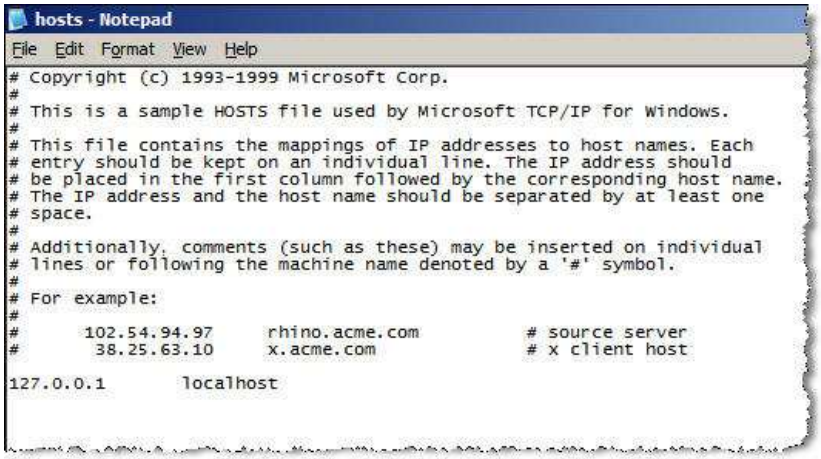
Phishing a Pharming

Pharming

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



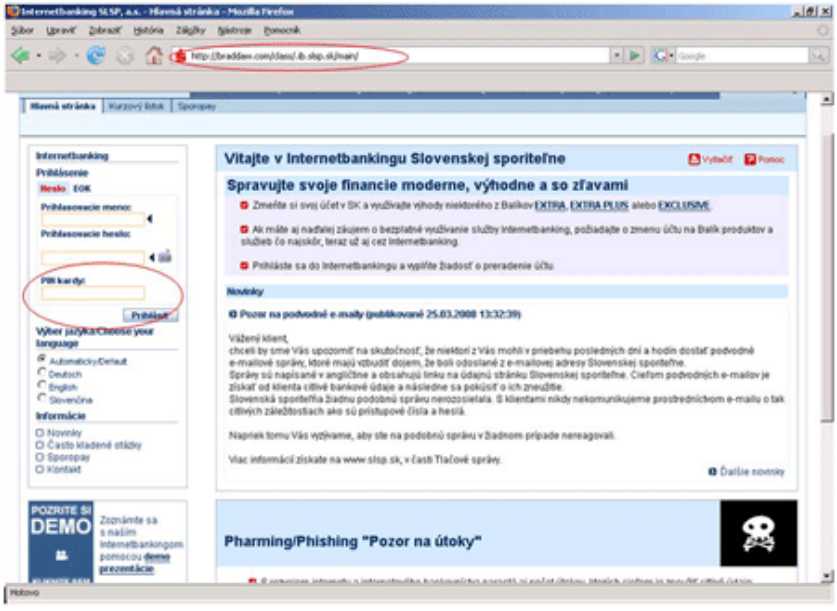
Pharming



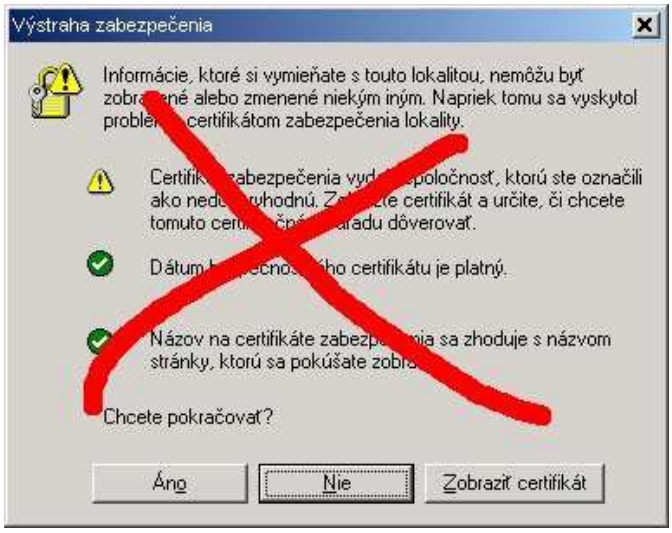
Ako odhaliť phishing a pharming?

- 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?

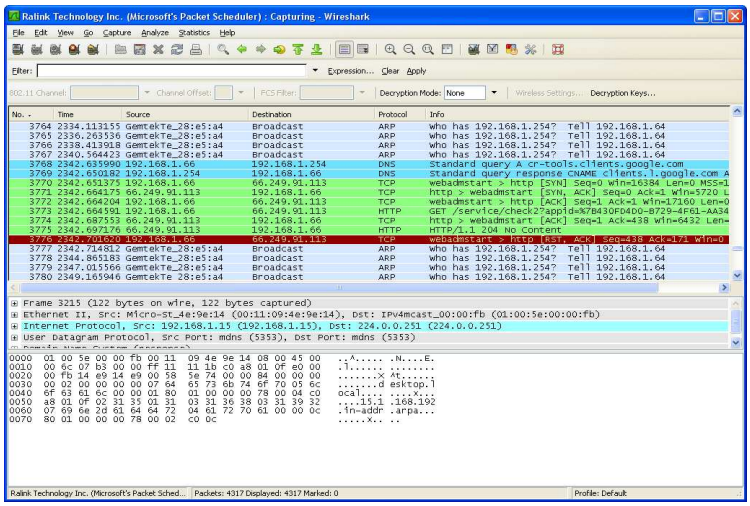


Ako odhaliť phishing a pharming?



sniffing

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

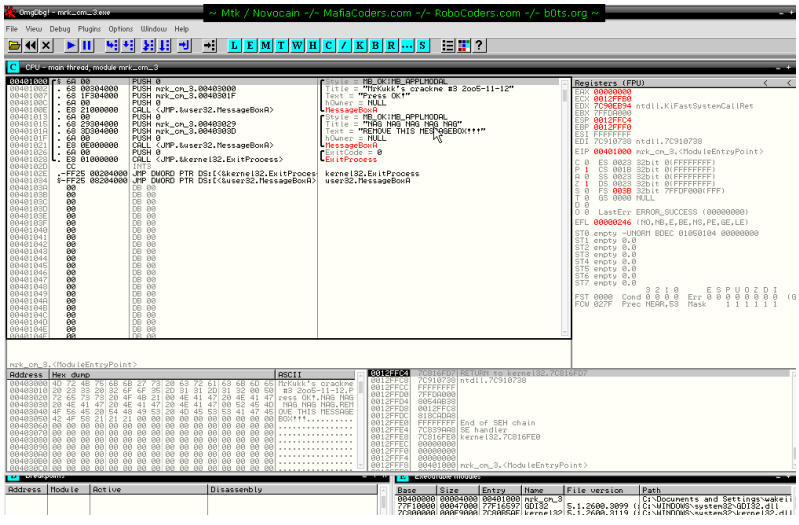


Opatrenia proti sniffing

- 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.



Cracking

Skimming

Skimming

Skimming

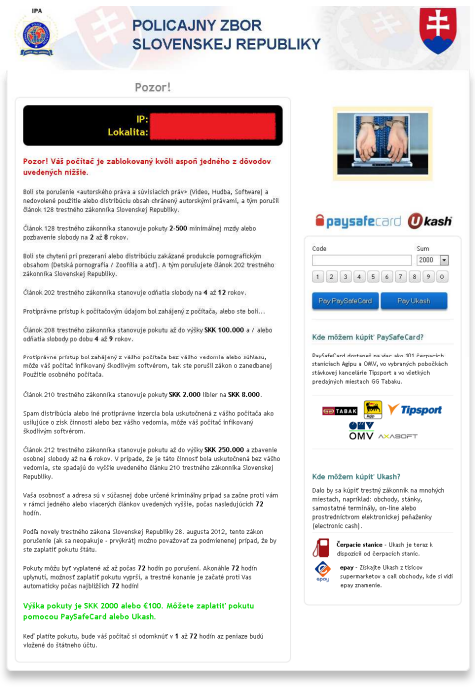
Škodlivý kód

- 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 obete.

Ransomware

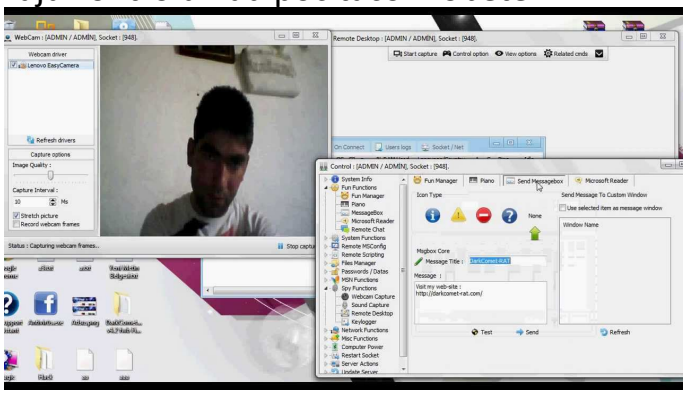
- druh škodlivého kódu, ktorým zločinci vydierajú užívateľov aby im zaplatili buď sumy pre fiktívny dôvody alebo priamo výkupné za ich dáta,
- tvári sa ako výzva štátneho orgánu na zaplatenie pokuty za spáchaný trestný čin alebo priestupok (porušenie autorských práv, nedovolená distribúcia detskej pornografie,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

Ransomware



Malware rôzneho druhu

- páchatelia často využívajú neopatrnosť a dôveru užívateľov,
- prostredníctvom e-mailových správ odosielajú 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)

kontakt

kpt. Mgr. Marek Švarc,
marek.svarc@minv.sk,
Klapka: 09610/50143
Mobil: 0908/633184

mjr. JUDr. Zoltán Šťavnický,
zoltan.stavnicky@minv.sk,
Klapka: 09610/50172
Mobil: 0917/648676

Ďakujeme za pozornosť!

OTÁZKY ?