Voľne šíriteľné nástroje na rozbitie hesiel.

Matúš Barabás

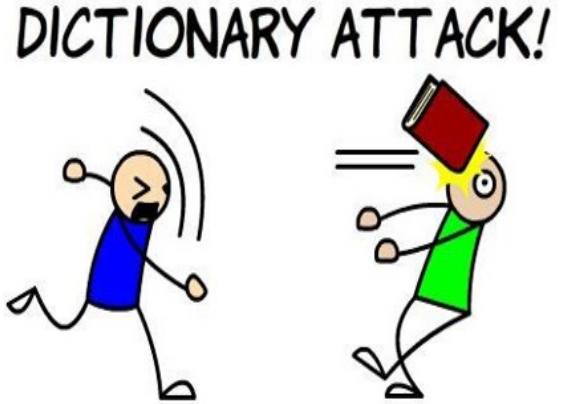
Obsah

Úvod

- Heslo – prostriedok autentifikácie používateľa
- 5 najpoužívanejších hesiel za rok 2016 – 123456, 123456789, qwerty, 12345678, 111111
- Bezpečnosť hesla
  - Sila hesla
  - Zabezpečenie na strane používateľa
  - Overovanie na strane systému
- Prelomenie/rozbitie hesla – proces získania hesiel z dát
  - Uložených na danom zariadení
  - Prenášaných prostredníctvom počítačových systémov

Dictionary attack (slovníkový útok)

- Systematické skúšanie hesiel z vopred pripraveného zoznamu – slovník
- Slovník – zoznam bežných slov – často používané ako heslá
- Úspešný aj pri kombináciách slov – predĺženie o niekoľko sekúnd
- Neúspešný
  - Náhodná kombinácia čísel a veľkých a malých písmen
  - Obmedzený počet pokusov zadávania hesla
- Rýchla metóda
- Efektívnejšia ako útok hrubou silou
- Nástroje - John the Ripper, L0phtCrack, Cain And Abel



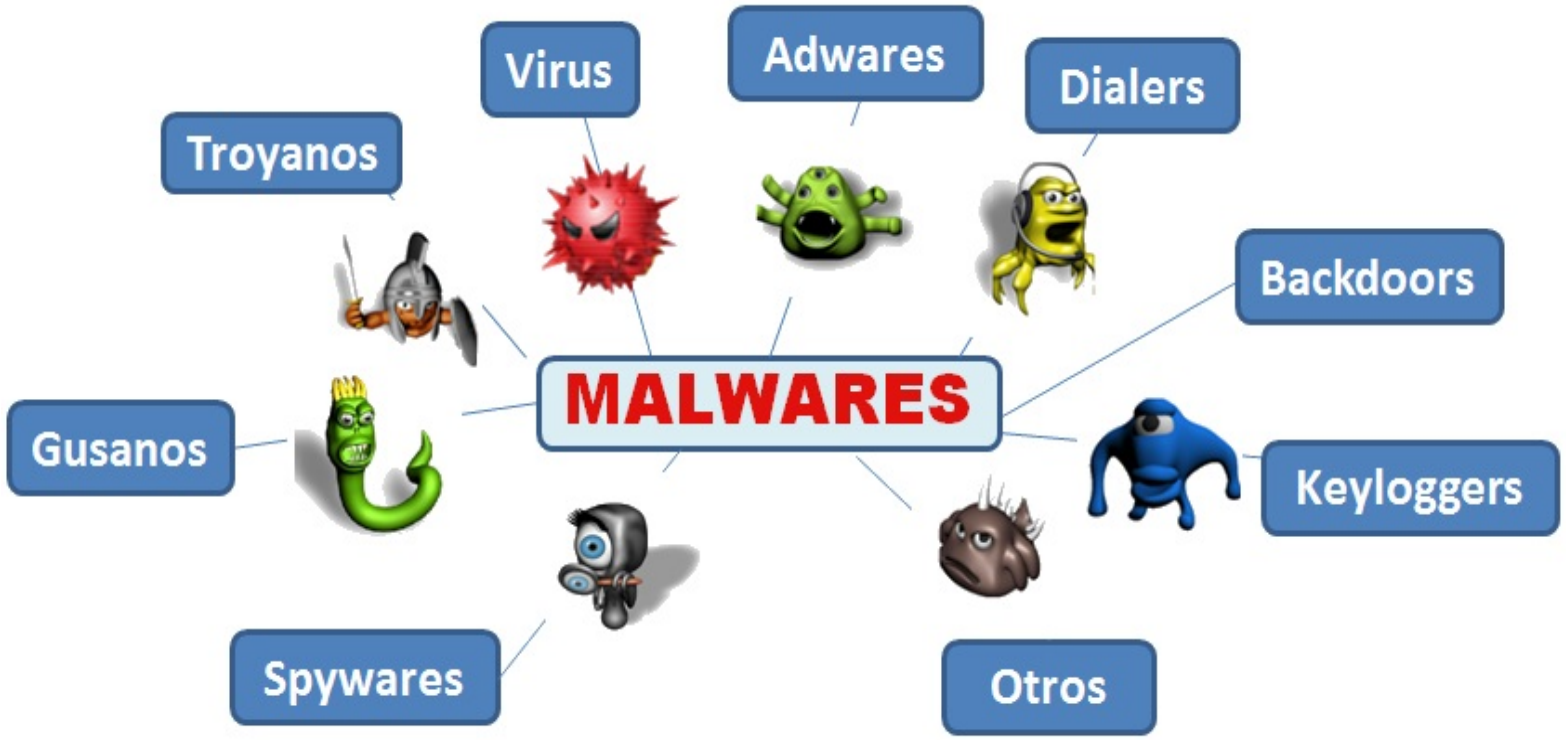
Phishing (krádež citlivých informácií)

- „Password fishing“ – doslovne rybolov hesiel
- Útočník – *„Phisher“*
  - Neoprávneným spôsobom získava údaje priamo od používateľov
  - Odosiela podvodný email – oznamuje zmenu alebo obnovenie účtu
  - Výstražné upozornenia v prípade neposkytnutia údajov
- Vytvorenie presnej kópie existujúcej dôveryhodnej stránky
- Ponúkanie výhod, ak sa prihlásia cez danú stránku
- Zadané prihlasovacie údaje po zadaní odoslané priamo útočníkovi

Malware (malvér)

- Všeobecné označenie škodlivého kódu
- Vírusy, trojské kone, spyware, adware
- Internet – slabá ochrana zabezpečenia stránok – preniknutie do počítača
- Po preniknutí do počítača malvér nainštaluje potrebný program, napr.
  - *„key logger“* – zaznamenáva text písaný na klávesnici
  - *„screen scraper“* – zaznamenáva obrazovku napr. v procese prihlasovania
- Malvér závisí na existencii webového prehliadača
  - Súbor, v ktorom sú uložené heslá používateľa
- Používateľ nemá ani potuchy, že sa niečo deje

Rozdelenie malvéru



Obr.: Toto sú typy existujúceho malvéru.

Rainbow table attack vs. Brute force attack

- Útok dúhovou tabuľkou
- Predvýpočítaná metóda – dúhova tabuľka obsahuje predvýpočítané hodnoty
- Vypočítava haš pre slová v slovníku – ukladá ho do dúhovej tabuľky
  - Porovnáva ho s hašom v dúhovej tabuľke – zhoda – heslo je prelomené
- Efektívnosť a časová náročnosť – závisí na veľkosti tabuľky a počte pozretí do nej
- OphCrack, RainbowCrack a iné

- Útok hrubou silou
- Prelomenie hesla bez znalosti kľúča
- Systematické skúšanie všetkých možných kombinácií malých, veľkých písmen a čísel
- Efektivita – závisí na dĺžke hesla
  - Do 6 znakov – efektívnejšia než slovníkový útok
  - Nad 6 znakov – rapídny pokles efektivity, nárast časovej náročnosti
- Čas – exponenciálne rastie s dĺžkou hesla
- John the Ripper

Primitívnejšie metódy prelomenia hesiel

Tab.: Tabuľka metód

Social engineering	Offline cracking	Shoulder surfing	Guess (hádanie)
Manipulácia ľudí s cieľom získať citlivé informácie	„Offline attack“ – útok uskutočňovaný bez prístupu na internet	Primitívnejšia metóda – aj tak môže priniesť mieru úspechu	Najlepší priateľ hackera – predvídateľnosť
Útočník neprichádza do osobného kontaktu s používateľom	Závisí na prístupe k súboru – obsahuje haše hesiel	Útočník – človek vydávajúci sa za kuriéra, servisného technika atď., aby získal prístup do budovy	Generovanie hesiel
Podvodný telefonát	Priamo v systéme používateľa	Člen firmy – dostáva od ostatných zamestnancov určitý druh voľného priechodu	Sledovanie a podrobná analýza používateľa
Útočník sa vydáva za IT bezpečnostného technika alebo inú zodpovednú osobu	V systéme, na ktorý má daný používateľ lokálny prístup	Zapisuje si poznámky nalepené na monitoroch zamestnancov	Útočník získa malý počet často úspešných potencionálnych hesiel
Vopred zistená pravdivá informácia (dátum narodenia, meno nadriadeného)	Jediná vec, ktorá mu môže zabrániť – limit daného hardvéru	Sleduje zamestnanca pri zadávaní prihlasovacích údajov	Útočník sám skúša pár pokusov o prihlásenie
Na základe informácií žiada citlivé údaje	Čím výkonnejší procesor – útočník môže vykonávať viac pokusov za sekundu	Dnešná moderná doba – skryté miniatúrne kamery a mikrofóny	Dostatočne podrobná a prepracovaná analýza – prelomenie hesla

Zabezpečenie hesiel

- Pre každý z dôležitých účtov používať jedinečné heslá
- Zapisovanie hesla – uchovať na tajnom neviditeľnom mieste
- Sila hesla závisí na
  - **Dĺžke** – dlhé hesla sú ťažšie prelomiteľné
  - **Zložení** – veľké a malé písmená, čísla a symboly
- Odborníci radia – určiť nejakú bežnú frázu – vziať začiatočné písmená – vytvorenie hesla
- Nastavenie rôznych možností hesla – pri obnove stále aktuálny mail ...
- Pravidelná aktualizácia hesiel

Zdroje

- Hande, Rohan. (2012). [online] Password Cracking – Part 4 – Online vs. Offline Password Cracking. Available at: http://rohanhande.blogspot.sk/2012/03/password-cracking-part-4-online-vs.html.
- Jančích, Vladimír. (2017). [online] Zase tie isté chyby. Toto sú najpoužívanejšie heslá v roku 2016. Available at: http://www.zive.sk/clanok/122375/zase-tie-iste-chyby-toto-su-najpouzivanejsie-hesla-v-roku-2016.
- Rouse, Margaret. (2005). [online] Dictionary attack. Available at: http://searchsecurity.techtarget.com/definition/dictionary-attack .
- Rouse, Margaret. (2017). [online] Password. Available at: http://searchsecurity.techtarget.com/definition/password.
- Šenkýrová, Lenka. (2013). [online] Čo je PHISHING alebo ako sa nestať obeťou podvodníkov. Available at: https://www.slsp.sk/sk/otazky-a-odpovede/co-je-phishing.
- Winder, Davey. (2011). [online] Top ten password cracking techniques. Available at: http://www.alphr.com/features/371158/top-ten-password-cracking-techniques.