Malware vtedy a dnes

Peter Košinár
kosinar@eset.sk

15. mája 2012

Čo dnes uvidíme?

1. Škodlivý softvér
2. Počítače okolo nás
3. Zákon a (ne)poriadok

Čo?

A čo si vy, Kefalín, predstavujete pod takým pojmom “malware”?

- Snaží sa nás obrať o majetok, dáta, . . .
- Zväčša funguje bez súhlasu používateľa (ale: PUA).
- Dostupný aj vo vašom meste!

Načo?

Škodlivý softvér nerastie na stromoch, vždy je za ním človek:

- Vlastný zisk (priamo, ale aj cez “služby” – spam, CC, . . .).
- Sláva a popularita.
- Svetonázor (politika, náboženstvo, . . .).
- Komerčná a štátna špionáž (Aurora, Stuxnet, . . .).

Skadiaľ?

Kde sa dá prihlásiť za obeť?

- E-maily – od “Kuk sem!” až po “Nech sa páči!”
- Web – hľadanie “zaujímavého” obsahu, . . .
- Bezpečnostné diery v programoch.
- Slabé heslá stále živé.

Bezpečnostné chyby

Microsoft Security Bulletin MS11-083 - Critical Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)

This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker sends a continuous flow of specially crafted UDP packets to a **closed** port on a target system.

Sláva


Smoke GANJA
Gymnazium Jamesa Hetfielda
Gymnazisti, aj tak sme vas dostali, h00116aNs
But the ganga crumbled and you've left with just a name
Where's your crown? King nothing***

Hanba

nbusr123 je jedno z najbezpečnejších hesiel na tejto planéte (prvé v tomto rebríčku je Chuck Norris).
Heslo vzhľadom na jeho vysokú bezpečnosť používa veľa orgánov štátnej správy: Národný nebezpečnostný úrad, IT špecialisti (títo ho však občas zvyknú zabudnúť, preto ho majú napísané na lepiacom štítku na monitore) a mnoho ďalších.
Odporúčania počítačových odborníkov po celom svete hovoria, že úplne najbezpečnejšie použitie hesla nbusr123 je v kombinácii s loginom nbusr, ako to demonštroval národný nebezpečnostný úrad na svojich serveroch, dokým na to neprišli zlí hackeri a NBÚ bolo nútené heslo zmeniť.

Ryby, rybky, rybičky, . . .

Date: Mon, 7 May 2012 07:34:28 +0200
From: "rosemerig@pmpf.rs.gov.br"
<rosemerig@pmpf.rs.gov.br>
Subject: Aktualizujte svoj účet Limit

Aktualizujte svoj účet Limit

Vaša poštová schránka prekročila jeden alebo viac veľkostnej limity stanovené správcom. Nemožno odosielať alebo prijímať e-maily, kým si veľkosť poštovej schránky sa znižuje. Ďalšie miestnosti. Prosím, kliknite na odkaz nižšie vyplniť a odoslať dáta s ľahkosťou.

http://uniba-sk.webs.com/contact.htm

Vďaka a ospravedlňujem sa.
Správca systému.

E-mail

From: illegal@fbi.gov
To: helmut@sajrajt.von
Subject: Illegal content
Date: Fri, 1 Apr 2012 03:13:37 +0200

You have been downloading illegal content!
See the attached list for details.

Attachment: server_logs.txt .exe

Hľadanie obsahu na nete

- Pornografia – klasický ťahúň.
- Warez – “Avatar 3D-HD.exe”, . . .
- Drive-by a nabúrané stránky.
- Bundling.

Nasledujúce zábery nie sú vhodné pre slabšie povahy.

???


Wet kitty wants to know what you typed into the search bar...

Háveď

Čo všetko môže počítač chytiť?

- Nenápadný lúčny, err, trójsky koník.
- Parazitické vírusy (súbory, dokumenty, . . .).
- V poslednej dobe je veľa vydieračov.

Vydieranie, vydieranie, to bude môj koníček. . .

Obrana?

Ako sa dá proti tomu brániť?

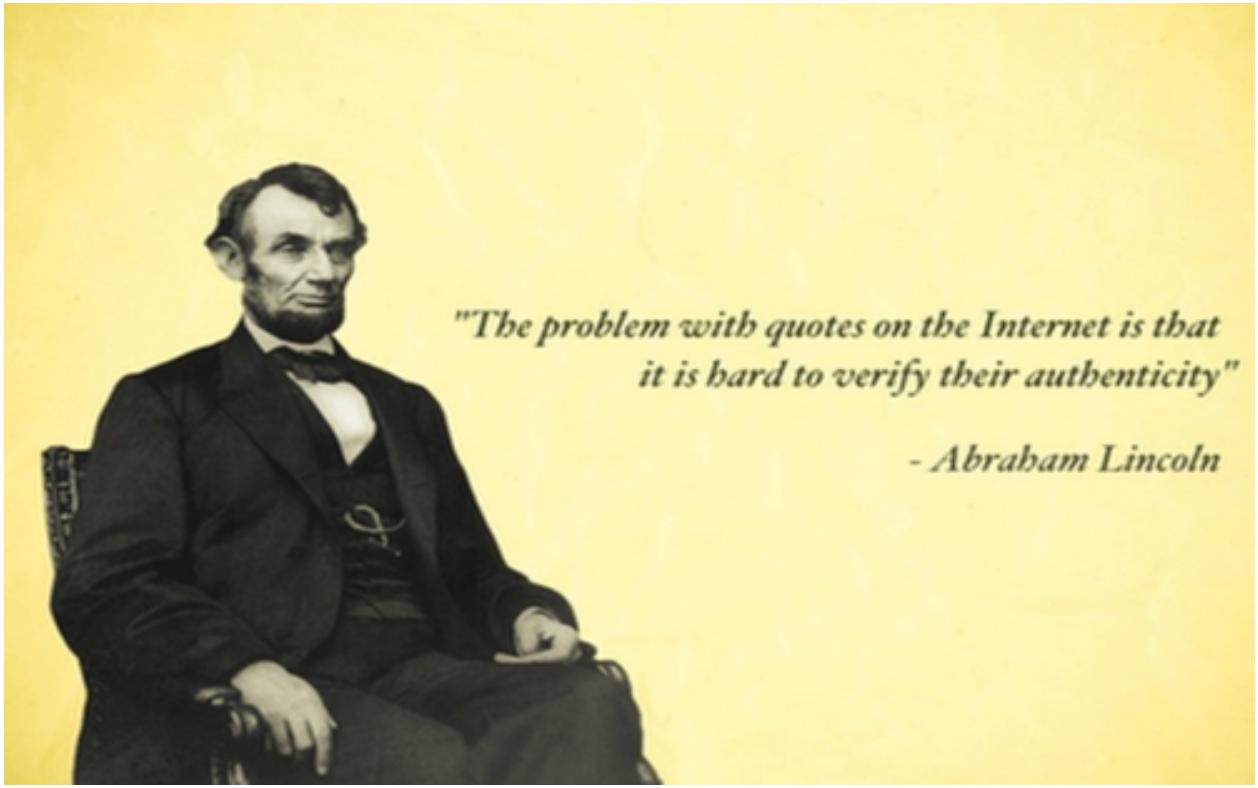
- Slovníkové heslo – metla ľudstva (ale pozor na DoS).
- Poznaj svojich známych (FB, LinkedIn, . . .)!
- Firewall pre pocit sucha a bezpečia (HTTP/UFBP).
- Zdravý rozum pomáha najviac.

Počítače okolo nás.

Kto počíta?

<unknown author>

"It took the computing power of 3 Commodore 64 to fly to the Moon."

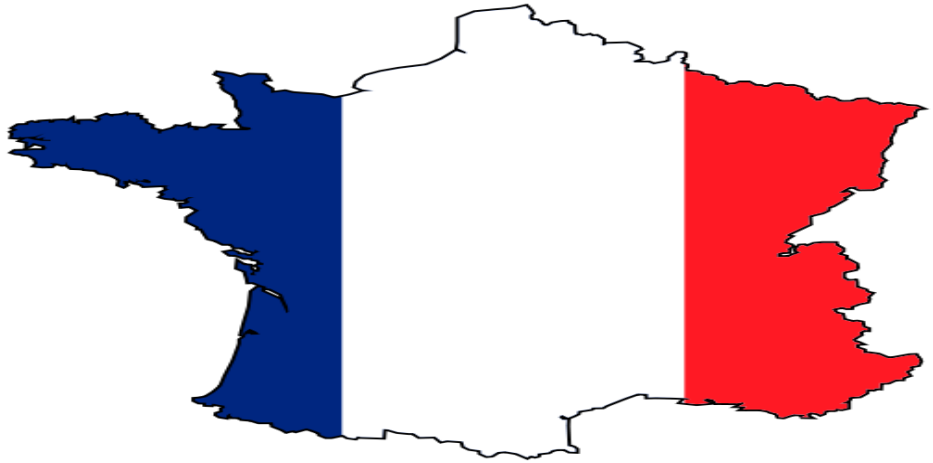

"The problem with quotes on the Internet is that
it is hard to verify their authenticity"
- Abraham Lincoln

Tak

Takže, kto to vlastne počíta?

- Mobily.
- Modemy.
- Tlačiarne.

SVK:FRA



Aký je stav?

Walker – Texas Ranger

Kto môže konať? Polícia. ALE:

- Zber informácii vs. súkromie?
- Globalizácia.
- Počítač nemôže ísť do basy.

Poriadok

Dobré správy:

- Slovenský poker-bankár.
- Carberp gang (`http://www.lifenews.ru/news/86143`)

To je už všetko!

Ďakujem za pozornosť! Ak sú otázky, sem s nimi! [1]

[1] Máte tiež právo mlčať, ale potom vaše otázky zostanú nezodpovedané.