



DÍRY, NEDÍRY...

Škodlivý software - malware

Co zajímá hackery (útočníky)

- hesla, přístupové certifikáty, atd.,
 - *například do banky, e-maily, facebook...*
- citlivé dokumenty s osobními či firemními informacemi
 - *použitelné pro vydírání/poškození firmy*
 - *filmy a hudba, kontakty,*
- zdroje počítače
 - *místo pro uložení cizích dat,*
 - *čas procesoru, ...*

Co zajímá hackery (útočníky)

- počítač může fungovat jako zombie
 - *počítač je vzdáleně ovládaný bez vědomí majitele:*
 - obvykle k nezákonným účelům – nevyžádaná pošta - spam
 - DDoS útoky (účelem je kolaps vybraného serveru)
 - *zákeřná snaha zničit co se dá*
- poslední době může sloužit jako rukojmí
 - *Zablokování OS*
 - *prostřednictvím vyděračského softwaru (ransomwaru).*

Děravý systém

- Jak se dostane malware se do systému?:
 - *Přes bezpečnostní nedostatky v OS*
 - *Přes bezpečnostní nedostatky v SW (Adobe Flash, ...)*
 - *e-mailly*
 - Obvykle spíše v jeho přílohách
 - Odkazy na různé nebezpečné webové stránky
 - *Přes různé komunikátory (Skype, Facebook apod.)*

Děravý systém

- Jak se dostane malware se do systému?:
 - *Freeware, shareware*
 - *Cracknuté aplikace*
 - *Nelegální OS Windows*
 - *aktivátory OS*
 - *...*

Děravý systém

- *Z pochybných webových stránek*
 - Nabídky aktualizací Adobe Reader, Adobe Acrobat, Flash Player, Apple QuickTime...
 - Upozornění že Váš systém je zavirován – nabídka skenování a odvírování
 - Upozornění že Váš systém obsahuje bezpečnostní díry – nabídka řešení
 - VŽDY ODMÍTNĚTE A UPALUJTE PRYČ

Děravý systém

- *Infikovaný USB flash disk*
 - AutoPlay – služba spouští automaticky SW na USB
- *Infikovaný software (freeware, cracknuté programy)*
- *Přes špatně zabezpečené síťové rozhraní*
- *atd.*

Podvodný e-mail - phishing



Podvodný e-mail - phishing

Soubor Úpravy Zobrazit Historie Záložky Nástroje nápověda

SERVIS 24 login - Ceska Sporitelna x +

← → ↻ 🏠 ⓘ 🔒 https://help-lolo.cf/SERVIS/online.htm| ● ● ●

SERVIS•24
INTERNETBANKING 956 777 956

Přihlášení SERVIS 24


Heslem Klientským certifikátem

[První přihlášení](#)

Klientské číslo

Heslo

[Zapomenuté/zablokované heslo](#)

 [Klávesnice](#) [? Návod k přihlášení](#) **Přihlásit**

To není platná adresa
Servisu.24 !!!

Podvodný e-mail - phishing

Varovani pred novou verzi podvodnych e-mailu

Ceska sporitelna [csas@servis24.cz]

Zpráva byla předána dál dne 12.3.2008 8:22.
V této zprávě byly odebrány nadbytečné konce řádků.

Komu: redakce@podnikatel.cz

Vazeni klienti,

radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas@csas.cz.

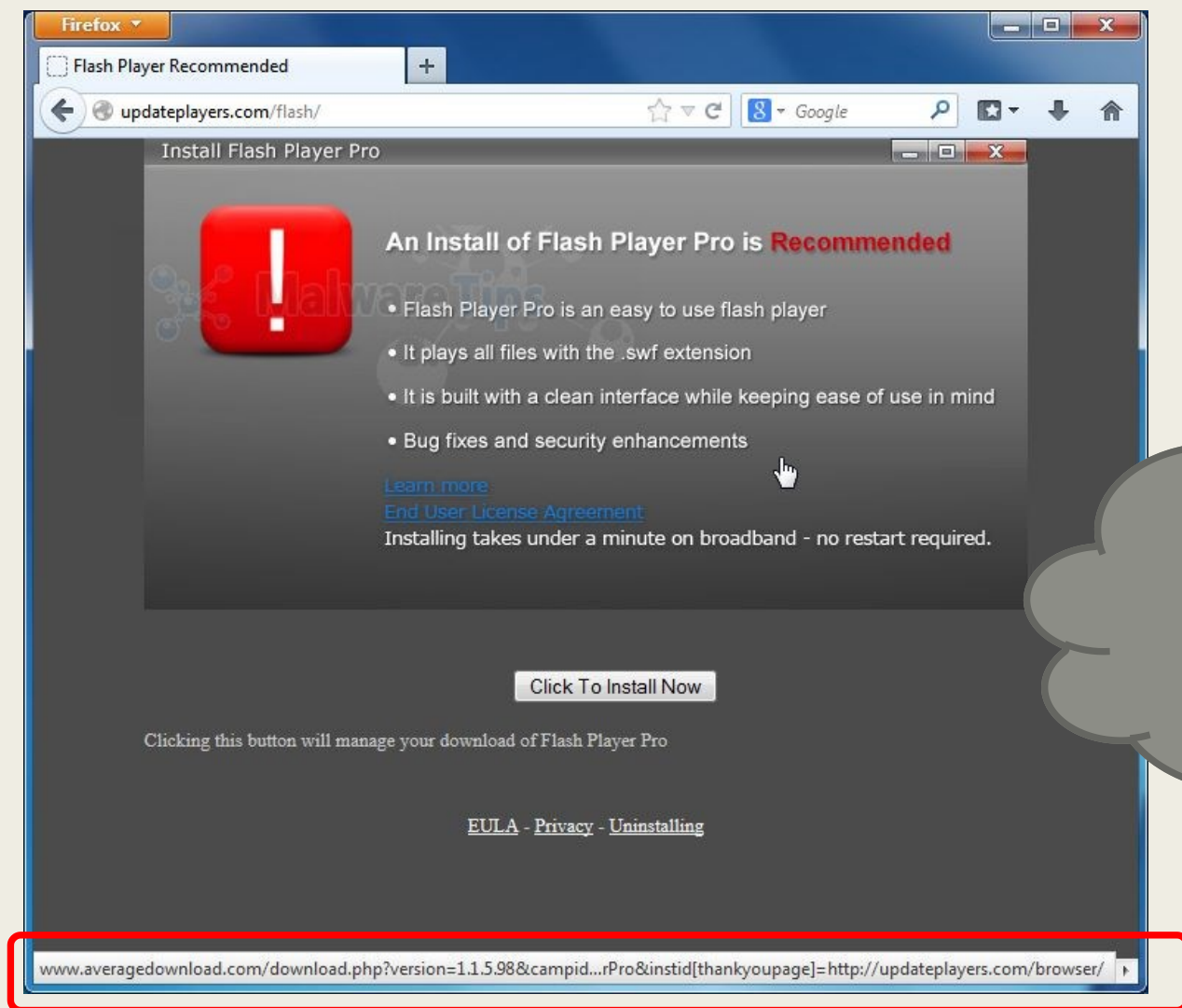
Obsahuje odkaz v tele na udajne webové stránky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju.

Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize:

<http://221.133.24.68:90/www2.servis24.cz/ebanking-s24/dispatcher.php?aid=19101203&lang=cs>

Verifikovaci spojeni je platne do 24 hodin.

Virus Flash Player



To není platná adresa
Firmy Adobe !!!

Virus Scanner OnLine

The screenshot displays the E-Set Antivirus 2011 user interface. The left sidebar contains navigation links: Overview, Scan PC (highlighted), License, Update, and Help. The main area is titled 'Scan for threats' and features two primary actions: 'Full computer scan' (described as using the full service scan to check everything) and 'Remove threats' (described as detecting, removing, and blocking all types of spyware and adware threats). Below these actions is a table listing detected threats.

File Name	Threat	Alert level	Status
C:\Program Files\Outlook Express\...	Keylogger.iSna...	High	Active
C:\Program Files\Windows NT\hyp...	Backdoor.POIS...	Medium	Active
C:\WINDOWS\system32\UninstallKB9683...	Trojan.Injector...	Medium	Active
C:\WINDOWS\assembly\NativeIm...	Email-Worm.Zh...	Critical	Active
C:\WINDOWS\assembly\NativeIm...	Spyware.BANK...	Low	Active
C:\WINDOWS\ie8\webcheck.dll	Trojan.Injector...	Medium	Active
C:\WINDOWS\ie8\updates\KB2416...	Email-Worm.Zh...	Critical	Active
C:\WINDOWS\system32\notepad....	Keylogger.iSna...	High	Active

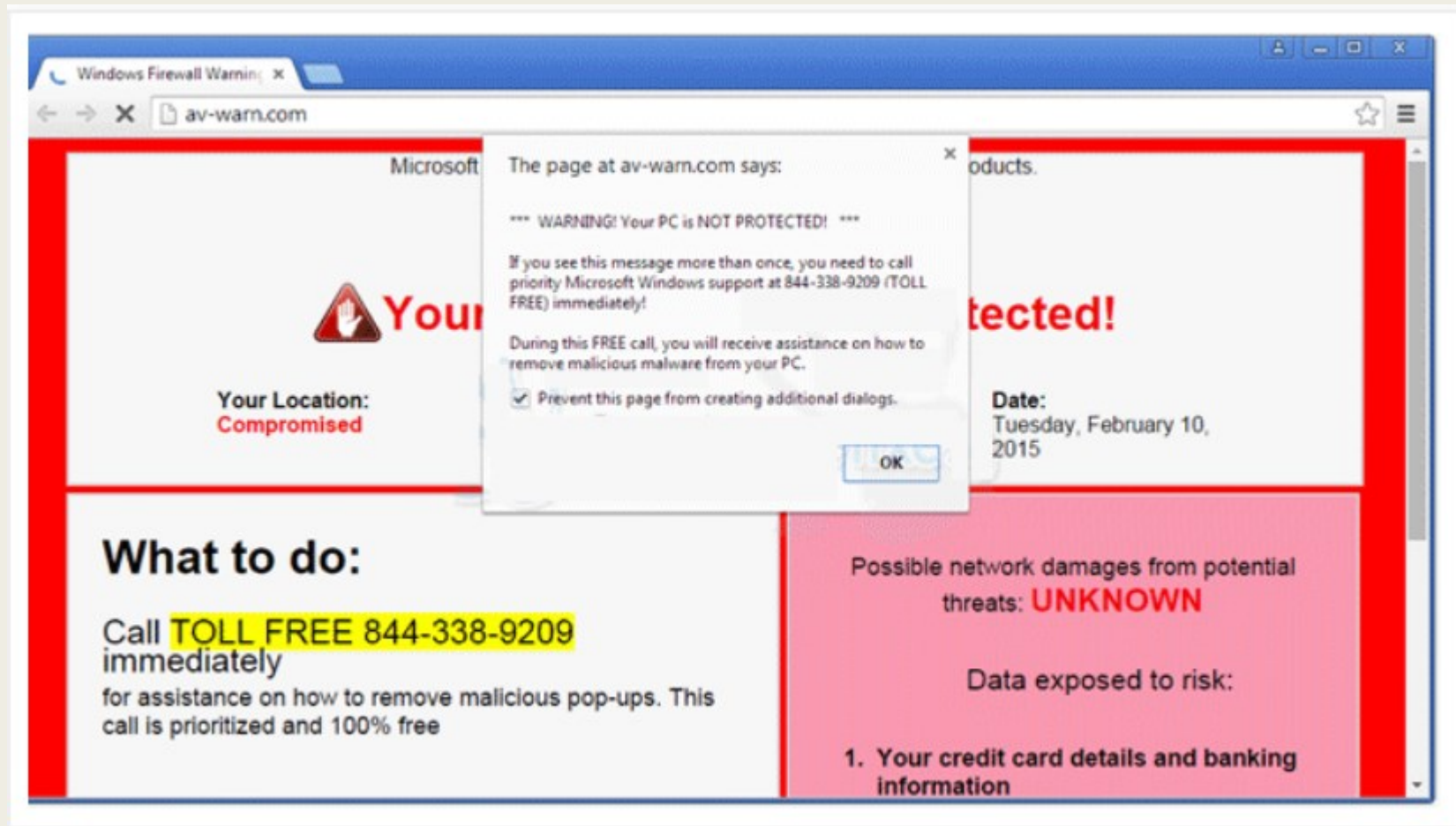
Below the table, a progress bar shows 100% completion. Scan statistics are provided: Start time: 11:23:56, Time elapsed: 1 minute(s) 02 second(s), Items scanned: -, Threats found: 22, and Item: -.

Statistics
Last scan: 17/03/11, 11:23
Last update: Never
Virus DB: 0.24.165.0t
Version: 4.9.1
License: Trial

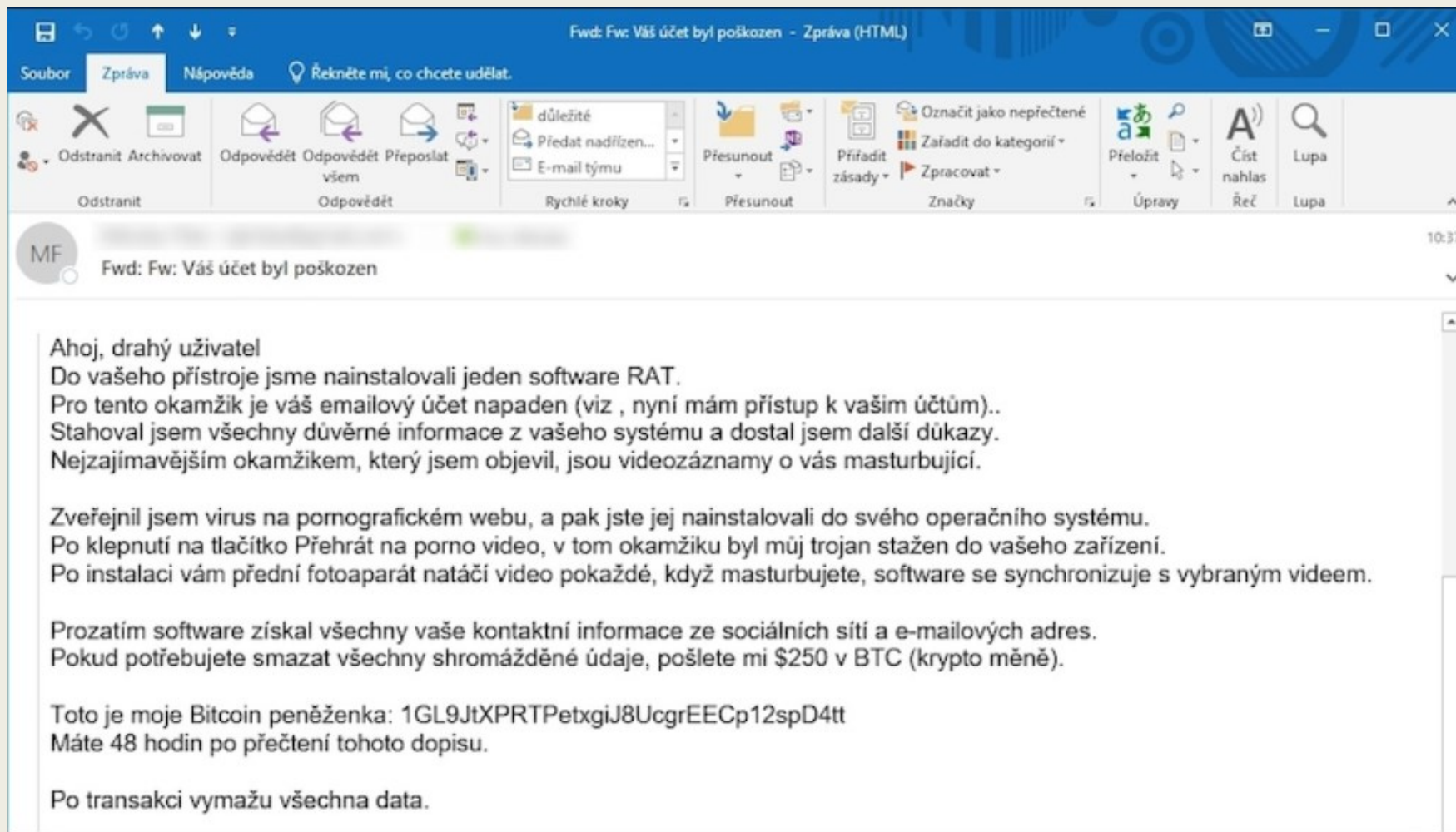
Virus Scanner OnLine



Virus Scanner OnLine



Vyděračské viry – ransom ware



Vyděračské viry - ransom ware



Ochrana dat a OS Windows

- **Pracujte pod uživatelským účtem**
 - Vytvořte „pracovní účet“ pro běžnou práci (internet, administrativa, zábava...)
- **Využijte maximálně ochranu: Řízení uživatelských účtů**
 - Nastavte **UAC** na max. úroveň, 100% funguje v uživatelském účtu
- **Používejte Firewall a antivirovou ochranu**
 - **Firewall:**
 - ochrana proti příjmu/odesílání **(ne)**známých dat **(ne)**známo kam
 - Ochrana proti ovládání PC „na dálku“
 - **Antivirová ochrana** (Windows Defender – dostačující)
 - Kontrola zda data/programy neobsahují škodlivý kód (malware)

Ochrana dat a OS Windows

- **Mějte vždy zaktualizovaný Antivirový program**
 - *Každým dnem přibývají nové viry a metody odstranění*
 - *kvalitní antivirus může hodně pomoci.*
- **Mějte vždy aktualizovaný operační systém**
 - *Každým dnem se hackeři pokouší nalézt nové „díry“ v OS*
 - *aktualizace řeší opravy zranitelností systému*
- **Používejte nejnižší nutná práva**
 - *Minimálně účet běžného uživatele*

Ochrana dat a OS Windows

- *Př. šifrovací virus zasáhne jen ta data, ke kterým máte přístup jako **uživatel/host***
- *Přístup s administrátorskými právy ohrozí všechna datová úložiště v **celém PC i vaší firemní/domácí síti**,*
- *zásah viru bude pro Vás/firmu ochromující.*
- **Kontrolujte, že jsou Vaše soubory v pořádku**
 - *Př. některé šifrovací viry pracují po napadení počítače co nejrychleji: během pár minut mohou zašifrovat všechna dostupná data*
 - *Jiné postupují pomalu a denně zašifrují jen pár souborů*
 - Tady je ještě šance nezašifrované soubory zachránit

Rozdělení malware

- **Backdoor** (zadní vrátka)
 - Ovládání/využívání PC „na dálku“ - ze sítě (internetu)
 - Probíhá na pozadí – uživatel často nic netuší
- **Ransomware** (vyděračské viry)
 - Často zašifrují data, za úplatu odšifrují
- **Phishing** (podvodné e-maily)
 - Např. snaha o získání údajů k přístupu k bankovním účtům apod.
- **Scanning Virus**
 - Pokus nahrát **malware** do PC pod záminkou kontroly bezpečnosti OS
 - Účinné v administrátorském účtu

Rozdělení malware

■ Rootkit:

- *Původně: sada nástrojů pro získání administrátorských oprávnění*
- *Dnes: nástroje maskující malware před systémovými nástroji/antiviry apod.*
- *Upravují OS tak aby malware nebyl zjistitelný*