Malware

PK-PT2 přednáška 5

České vysoké učení technické v Praze
Fakulta informačních technologií

Kategorie software a jejich detekce

Kategorie software z pohledu "škodlivosti":

- čistý škodlivý ostatní — co to je?

- **Kategorie software z pohledu detekce AV nástroji:**
- nedetekovaný
- detekovaný jako
- malware detekovaný jako PUA

Co je mezi čistým a škodlivým softwarem?

- “Grayware”
- “PUA” (Potentially Unwanted Application; též PUP — Potentially Unwanted Program, apod.)

Grayware

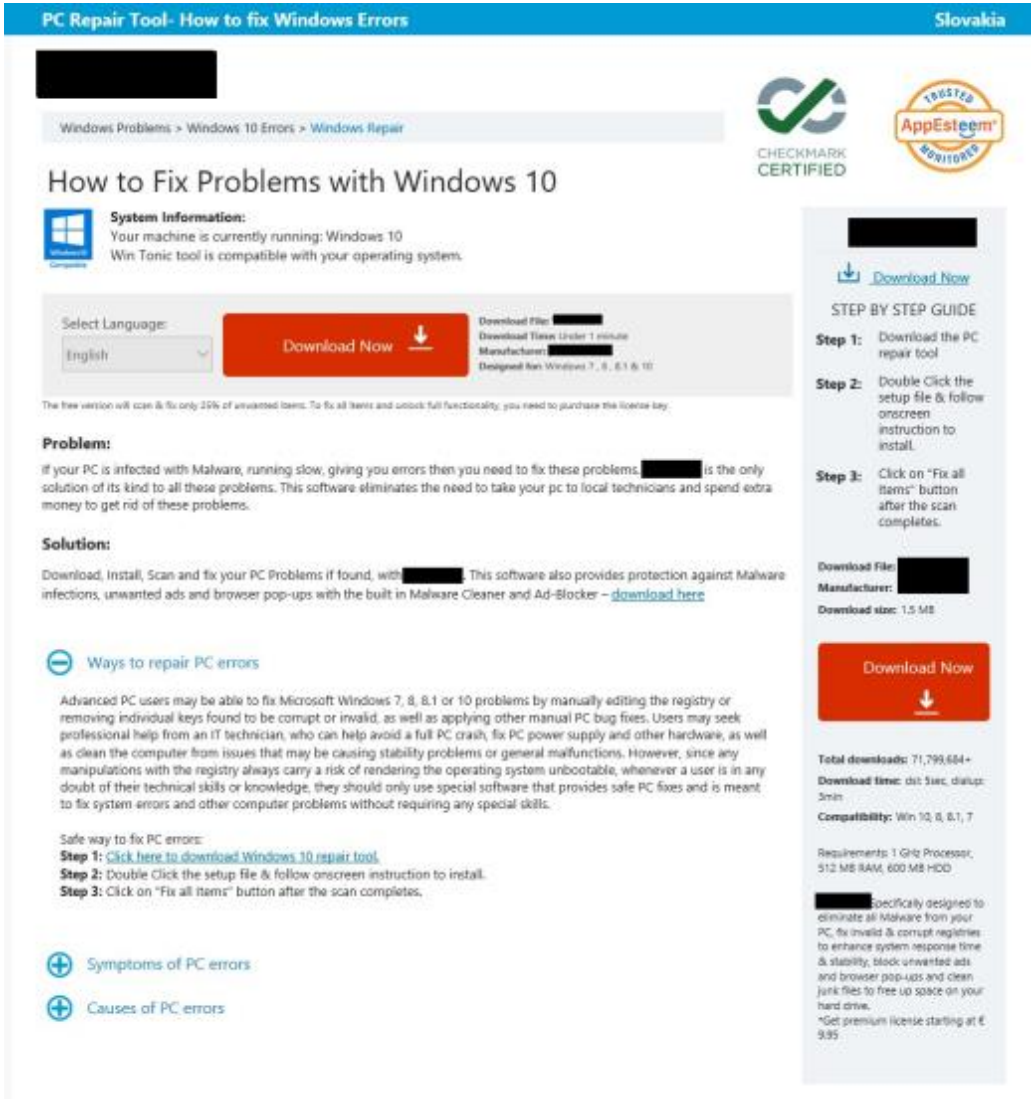
Software, který není vysloveně škodlivý, ale také nelze označit za jednoznačně legitimní.

- software, který uživateli zobrazuje nevyžádanou reklamu software,
- který uživateli lže nebo mu poskytuje zavádějící informace čističe registrů nebo optimalizátory výkonu pro Windows v minulosti např. nástrojové lišty do prohlížečů
-

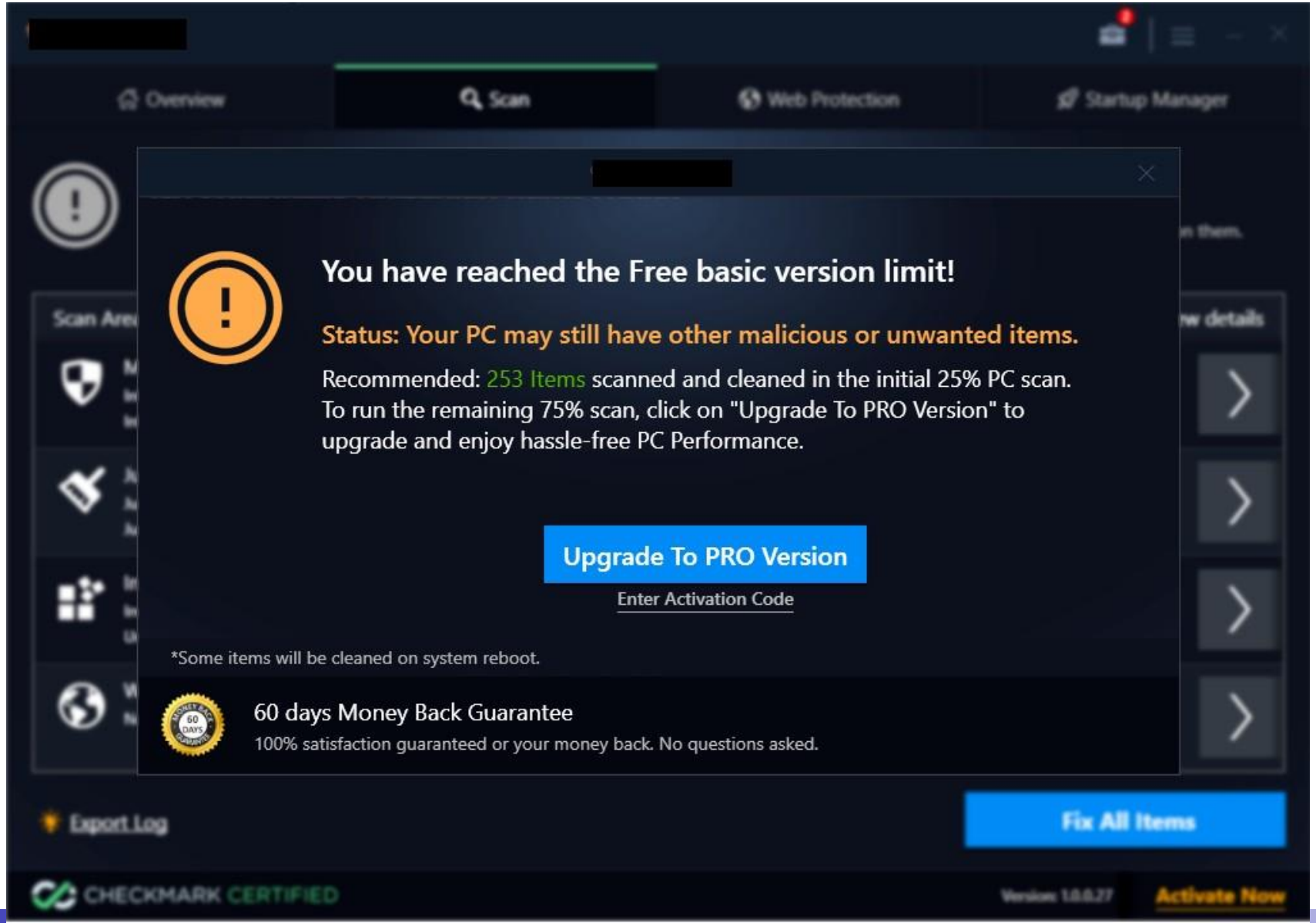
software, který používá nelegální nebo neetické obchodní praktiky k tomu, aby přiměl uživatele, aby si ho nainstaloval, přestože vlastně nechce tzv. bundleware (software přibalovaný k jiným aplikacím) tzv.

- download wrappery software propagovaný nebo distribuovaný pomocí
- zavádějících URL (např. `https://www.microsoft.com-`
- `some.other.domain.com/`). software, který se snaží přesvědčit uživatele, že je legitimní, podobou se skutečně legitimním software
- software, který se tváří jako zdarma, ale pokouší přimět uživate, aby nevědomky zaplatil
-

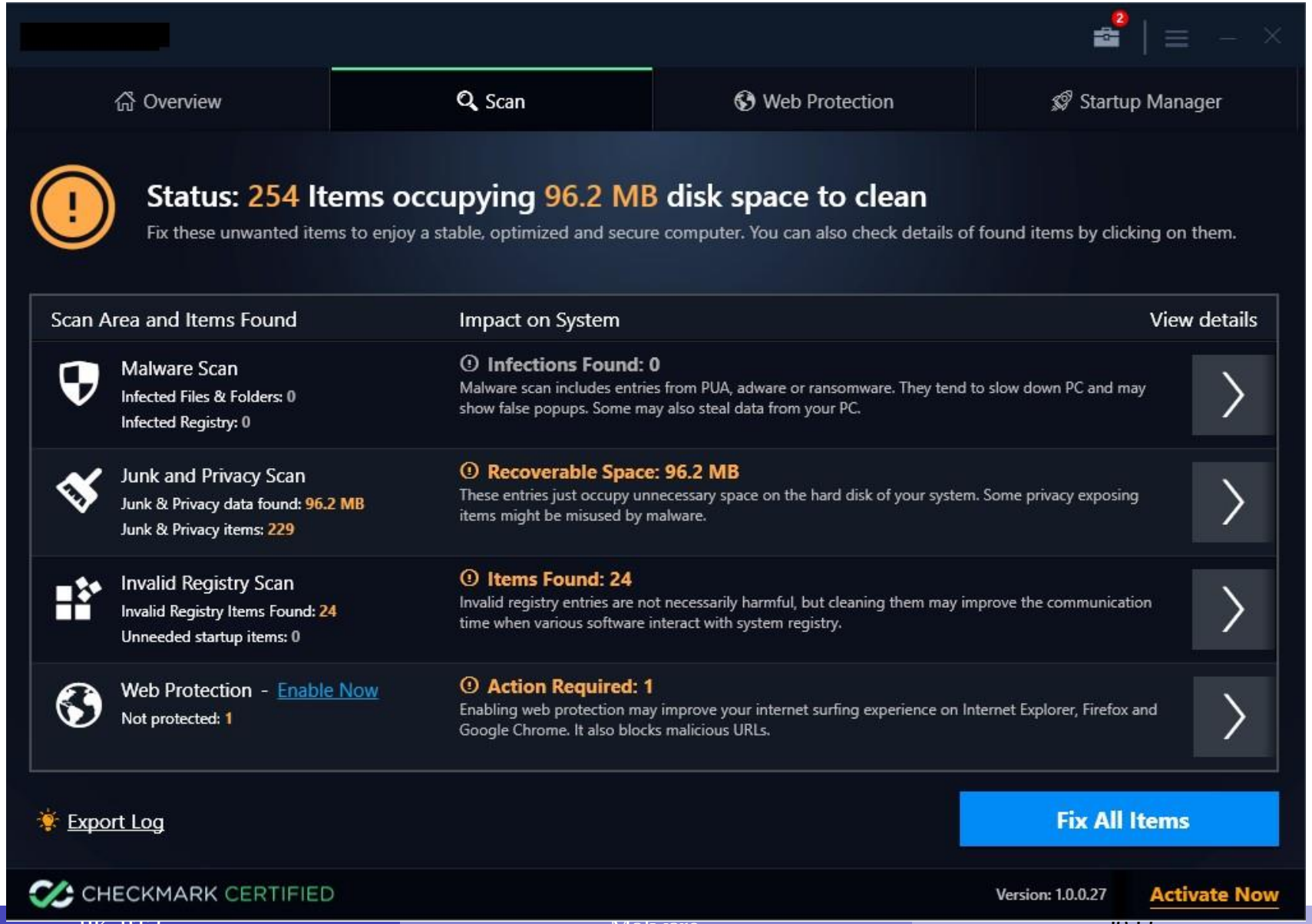
Grayware - příklad 1


PC Repair Tool- How to fix Windows Errors
Slovakia
[redacted]
Windows Problems > Windows 10 Errors > Windows Repair
How to Fix Problems with Windows 10
CHECKMARK CERTIFIED
AppEsteem
System Information:
Your machine is currently running: Windows 10
Win Tonic tool is compatible with your operating system.
Select Language:
English
Download Now
Problem:
If your PC is infected with Malware, running slow, giving you errors then you need to fix these problems. [redacted] is the only solution of its kind to all these problems. This software eliminates the need to take your pc to local technicians and spend extra money to get rid of these problems.
Solution:
Download, Install, Scan and fix your PC Problems if found, with [redacted]. This software also provides protection against Malware infections, unwanted ads and browser pop-ups with the built in Malware Cleaner and Ad-Blocker – download here
Ways to repair PC errors
Advanced PC users may be able to fix Microsoft Windows 7, 8, 8.1 or 10 problems by manually editing the registry or removing individual keys found to be corrupt or invalid, as well as applying other manual PC bug fixes. Users may seek professional help from an IT technician, who can help avoid a full PC crash, fix PC power supply and other hardware, as well as clean the computer from issues that may be causing stability problems or general malfunctions. However, since any manipulations with the registry always carry a risk of rendering the operating system unbootable, whenever a user is in any doubt of their technical skills or knowledge, they should only use special software that provides safe PC fixes and is meant to fix system errors and other computer problems without requiring any special skills.
Safe way to fix PC errors:
Step 1: Click here to download Windows 10 repair tool.
Step 2: Double Click the setup file & follow onscreen instruction to install.
Step 3: Click on "Fix all items" button after the scan completes.
Symptoms of PC errors
Causes of PC errors
[redacted]
Download Now
STEP BY STEP GUIDE
Step 1: Download the PC repair tool
Step 2: Double Click the setup file & follow onscreen instruction to install.
Step 3: Click on "Fix all items" button after the scan completes.
Download File: [redacted]
Manufacturer: [redacted]
Download size: 1.5 MB
Download Now
Total downloads: 71,799,684+
Download time: dsl 5sec, dialup 5min
Compatibility: Win 10, 8, 8.1, 7
Requirements: 1 GHz Processor, 512 MB RAM, 600 MB HDD
[redacted] specifically designed to eliminate all Malware from your PC, fix invalid & corrupt registries to enhance system response time & stability, block unwanted ads and browser pop-ups and clean junk files to free up space on your hard drive.
*Get premium license starting at € 9.95

Grayware - příklad 2


Overview
Scan
Web Protection
Startup Manager
You have reached the Free basic version limit!
Status: Your PC may still have other malicious or unwanted items.
Recommended: 253 Items scanned and cleaned in the initial 25% PC scan.
To run the remaining 75% scan, click on "Upgrade To PRO Version" to upgrade and enjoy hassle-free PC Performance.
Upgrade To PRO Version
Enter Activation Code
*Some items will be cleaned on system reboot.
60 days Money Back Guarantee
100% satisfaction guaranteed or your money back. No questions asked.
Export Log
Fix All Items
CHECKMARK CERTIFIED
Activate Now

Grayware - příklad 2


Overview
Scan
Web Protection
Startup Manager
Status: 254 Items occupying 96.2 MB disk space to clean
Fix these unwanted items to enjoy a stable, optimized and secure computer. You can also check details of found items by clicking on them.
Scan Area and Items Found
Impact on System
View details
Malware Scan
Infected Files & Folders: 0
Infected Registry: 0
Infections Found: 0
Malware scan includes entries from PUA, adware or ransomware. They tend to slow down PC and may show false popups. Some may also steal data from your PC.
Junk and Privacy Scan
Junk & Privacy data found: 96.2 MB
Junk & Privacy items: 229
Recoverable Space: 96.2 MB
These entries just occupy unnecessary space on the hard disk of your system. Some privacy exposing items might be misused by malware.
Invalid Registry Scan
Invalid Registry Items Found: 24
Unneeded startup items: 0
Items Found: 24
Invalid registry entries are not necessarily harmful, but cleaning them may improve the communication time when various software interact with system registry.
Web Protection - Enable Now
Not protected: 1
Action Required: 1
Enabling web protection may improve your internet surfing experience on Internet Explorer, Firefox and Google Chrome. It also blocks malicious URLs.
Export Log
Fix All Items
CHECKMARK CERTIFIED
Version: 1.0.0.27
Activate Now

Potentially Unwanted Application (PUA)

V zásadě neškodný a mnohdy zcela legitimní program, který však často bývá zneužívaný ke škodlivým účelům (tzv. “unsafe”):

- nástroje pro těžení kryptoměn ovládané z příkazové řádky aplikace
- pro vzdálený přístup k počítači

- nebo který používá techniky typické pro malware (tzv. “suspicious” :
- software, který zasahuje do standardního chodu systému (např. různé náhrady Start Menu pro Windows 10 nebo 11) nástroje pro podvádění ve hrách

  případně je často do počítače nainstalován bez skutečného souhlasu
- uživatele (tzv. “unwanted”).

Klasifikace malwaru

Malware lze rozdělovat do kategorií podle mnoha hledisek:

- podle způsobu šíření podle toho, kam se do
- počítače ukládá podle účelu, který sleduje podle
- způsobu, jak funguje podle programovacího
- jazyka, ve kterém je napsán
- ...
- Klasifikace malwaru — podle způsobu šíření

Virus — upravuje existující binární soubory tak, aby se jeho kód spustil místo nebo vedle původního kódu.

- **Worm** (červ) — propaguje kopie škodlivého souboru do dalších systémů rozesílá se mailem na adresy zjištěné z adresáře uživatele kopíruje se do zapisovatelných síťových adresářů
  - nahrává se na vložená vyměnitelná média
  - ...
- **Trojan** — šíří se jinak

Klasifikace malwaru — podle místa uložení

- do běžných souborů do zaváděcích nebo
- nevyužitých oddílů disku do dalších umístění
- (např. registry Windows) neukládá se
-

Klasifikace malwaru — podle účelu I

- **Adware**[1] — Zobrazuje reklamy na uživatelově počítači; může jít o zcela nové reklamy nebo o náhradu původních vlastními.
- **Backdoor** — Umožňuje počítač vzdáleně ovládat někým jiným než legitimním uživatelem.
- **Banker** — Útočí na používání elektronického bankovnictví. Může krást autentizační údaje (přihlašovací jméno a heslo, údaje z 2. autentizačního faktoru) nebo např. skrytě manipulovat s vkládanými údaji (těsně před odesláním příkazu k úhradě změnit číslo účtu a částku).

- **Coinminer** — Zneužívá dostupný výkon počítače k těžení kryptoměn pro útočníka.
- **Downloader** — Stahuje další aplikace (typicky další malware) a zajišťuje jejich spuštění.

Klasifikace malwaru — podle účelu II

- **Joke** — Obtěžuje uživatele, např. přehází znaky na klávesnici nebo otočí obrazovku vzhůru nohama. Jako malware je detekován v případě, že je pro běžného uživatele obtížné se ho zbavit.

- **Ransomware** — Šifruje uživatelská data a následně vydírá, aby uživatel zaplatil za jejich odšifrování.
- **Spy** — Krade data uživateli a předává je někomu jinému.
- **Agent** — Všechno ostatní.

[1]neplést s distribučním modelem stejného jména

Klasifikace malwaru — podle způsobu, jak funguje

- **Exploit** — Využívá veřejně známé i neznámé zranitelnosti v jiných programech k překonání bezpečnostních omezení.
- **Rootkit** — Manipuluje s daty operačního systému tak, aby skryl činnost či existenci malware.
- **Advanced Persistent Threat (APT)** — Provádí cílený útok na konkrétní oběť.
  - Vyhýbá se jiným než cílovým systémům.
  -
  -
  -

Využívá specifické znalosti o oběti.
Snaží se zůstat co nejdéle skrytý, např. potlačením podezřelých činností.
Často jde o vysoce pokročilý kód využívající informace, které jsou v té době neznámé nebo málo známé.

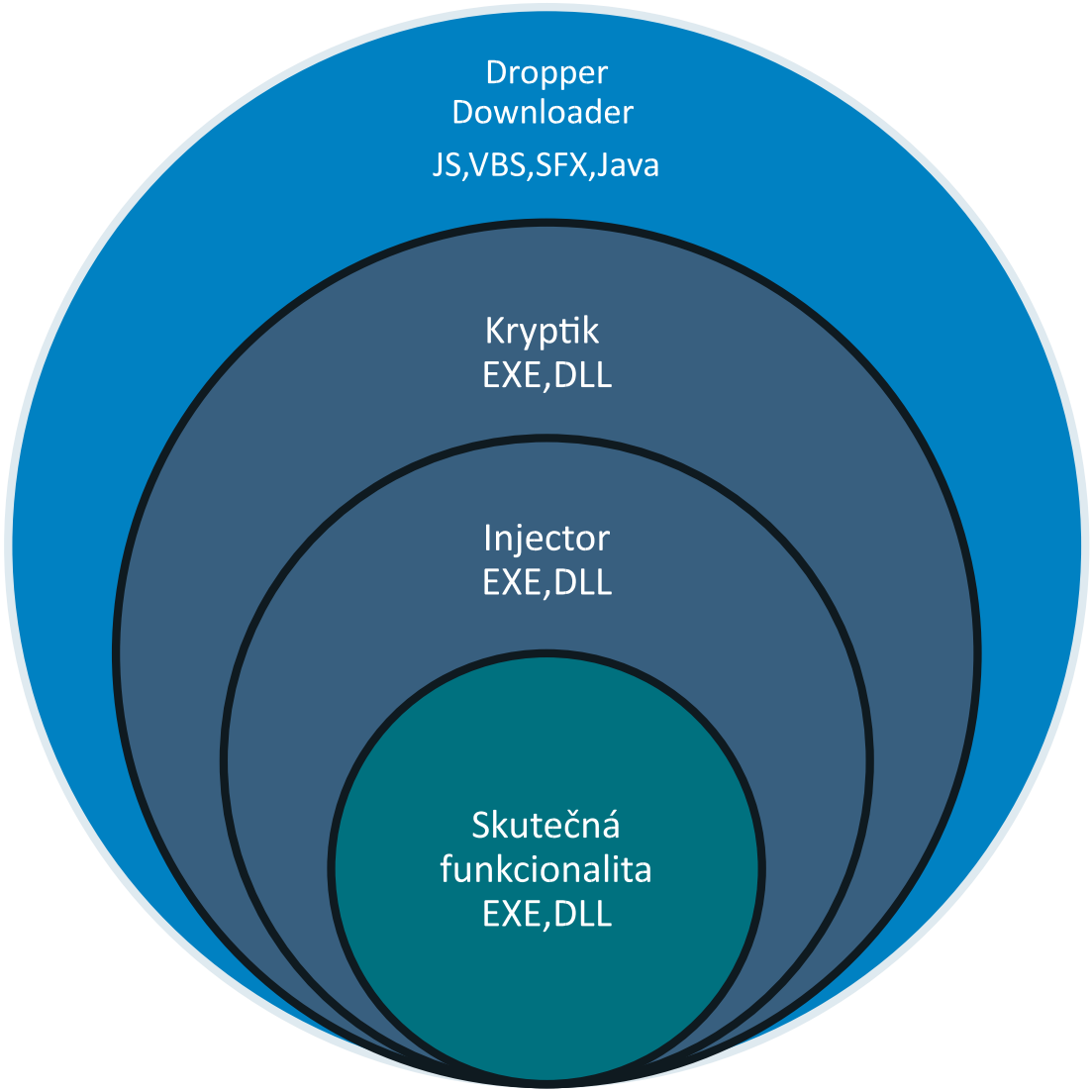
Charakteristiky moderního malware

- Je to business.
- Profesionalizace tvůrců.
- Variabilita v nainstalovaných instancích.
- Modularita.
- Komplexní struktura.

Tři cíle malware

- **Infekce** — proniknutí do cílového systému.
- **Persistence** — přežití v systému po dlouhou dobu.
- **Monetizace** — získání prospěchu pro tvůrce malware.

Typická struktura malware


Dropper
Downloader
JS,VBS,SFX,Java
Kryptik
EXE,DLL
Injector
EXE,DLL
Skutečná
funkcionalita
EXE,DLL

Downloader/Dropper

- Neprovádí škodlivou činnost.
- Cílem je uložit do systému další část malware — infekce.
  - Downloader — stáhne ji z internetu.
  - Dropper — vyextrahuje ji z dat dropperu.
- Může probíhat vícestupňově (dropper uloží na disk downloader, ten spustí, ten stáhne další downloader...).
- Může řešit i perzistenci.
-
  -
  -

Motivace:

Velmi rychle detekován antivirem (minuty až hodiny).

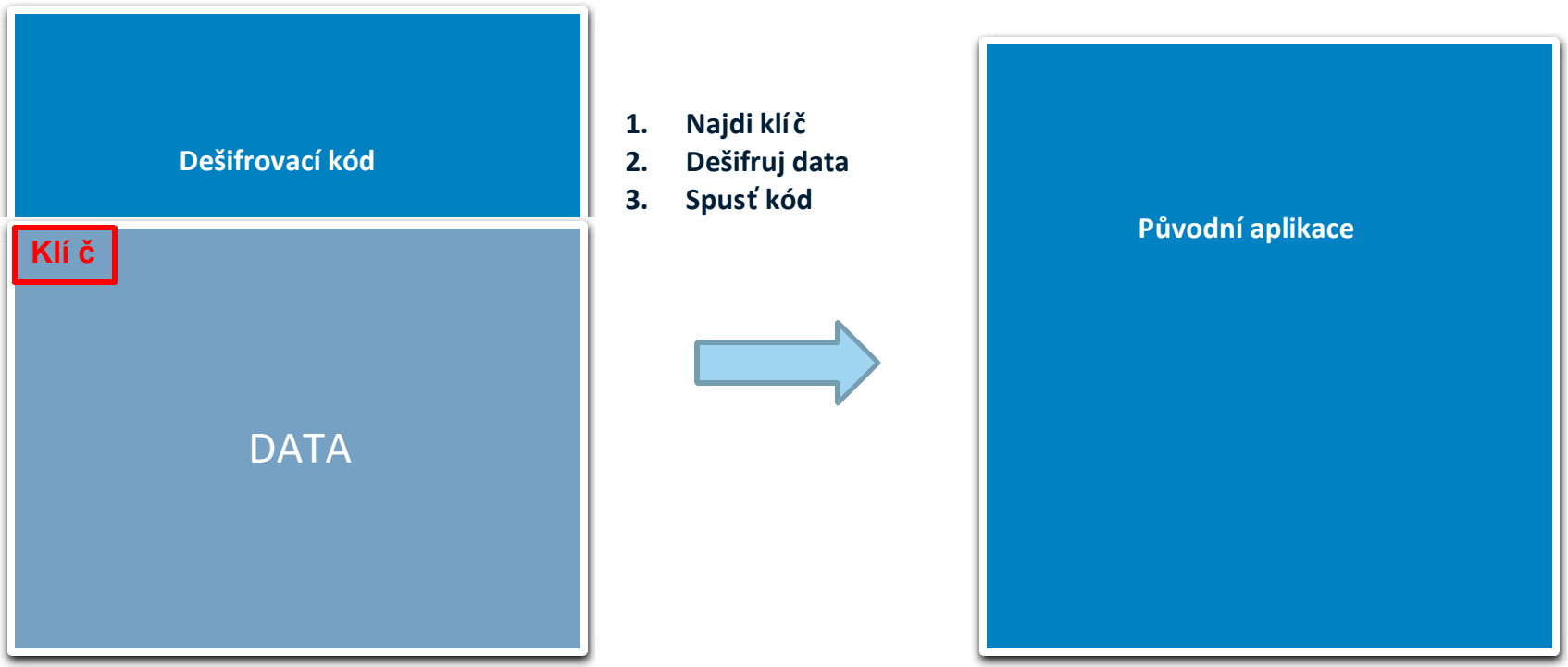
Velmi snadno modifikovatelný.

Kryptik

- Cílem je dosáhnout maximální variability malware.
- Řešení: Další vrstva malware je zašifrovaná, zkomprimovaná nebo jinak pozměněná tak, aby každá kopie byla odlišná (stačí změnit klíč).
- Problém: Takový kód ovšem nejde spustit.
-

Řešení: K zašifrovanému kódu je přiložena spustitelná “obálka”, která provede dešifrování a poté spustí původní kód.

Kryptik


Dešifrovací kód
Klí č
DATA
1. Najdi klí č
2. Dešifruj data
3. Spusť kód
Původní aplikace

Perzistence

- Cílem perzistence je zajistit, aby malware vydržel funkční dlouhou dobu.
- To znamená zejména:
  - Zajistit odolnost vůči restartu počítače.
  - Zabránit detekci běžnými nástroji.
  - Zabránit detekci antivirovými nástroji.

Odolnost vůči restartu počítače I

- Každý operační systém umožňuje automatické spouštění programů po restartu.
- Ve Windows například:
  - Speciální klíče v registru Windows:

Výběr registrů Windows pro automatické spuštění

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows
...

Speciální složky na disku:

`C:\Users\`*`uživatel`*`\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`

Odolnost vůči restartu počítače II

Plánovač úloh

Správce služeb

-
-
  - Skupinové politiky
  - Asociace k příponám souborů
  - ... a mnoho dalších (zkuste program **Autoruns**, součást **SysInternals Suite**).
- Nahrazení běžně spouštěné legitimní aplikace škodlivou.
- Nahrazení běžně načítané dynamické knihovny škodlivou.
- Startovací kód operačního systému ve vyhrazených sektorech disku.
- Startovací kód UEFI (velmi složité).
- ...

Skrývání malwaru a jeho činnosti

Minimálně je nutné zamezit tomu, aby byl malware vidět ve Správci

Použít nenápadné jméno pro program (velký red-flag pro antivirus):

Běžné jméno, ale umístěné v neobvyklém adresáři:
`C:\Windows\Temp\svchost.exe`

Běžné jméno s malou úpravou: `lssas.exe`, `Isass.exe`

Skrýt malware do dynamické knihovny, využít chyby v legitimní aplikaci pro načtení škodlivé knihovny namísto standardní.

Použít injekci — přesun kódu do jiného procesu.

- Použít rootkit — manipulace s datovými strukturami operačního systému, umožní skrýt malware před OS samotným i antiviry. Skrytí činnosti malware:
  - Obvykle značně obtížné a použitelné jen do první detekce.
  - Použití neobvyklých API?
  - Ve Windows manipulace s ETW (Event Tracing for Windows).

Obrana malwaru před antiviry nebo analýzou

- Spustit malware dvakrát, procesy se vzájemně kontrolují a pokud jeden
-
-
-
-
-

chybí, druhý ho spustí znovu.

Využít zámků při otvírání souborů k zabránění přístupu k souboru malwaru.

Připojit se sám k sobě jako debugger (ve Windows může být k procesu připojen pouze jeden debugger).

Manipulování se souborovými či procesovými API (detekce a přeskočení operace `DELETE` nad souborem malwaru).

Přerušit činnost, pokud je detekován běžící antimalware.

Odložit činnost na pozdější dobu.

Lze přežít formátování disku?

Ano, ale ne lehce.

- Infekce BIOS nebo UEFI základní desky.
- Infekce firmware jiné komponenty počítače.
- Infekce jiného počítače a pravidelná re-infekce všech počítačů na síti využitím nezáplatovaných chyb.

Pozor, některý malware perzistenci nepotřebuje - např. ransomware.

Monetizace

Monetizace I

- Monetizace (“převedení na peníze”) je hlavním cílem většiny malwaru.
-
-
  -
  -
  -
  -
-
  -
  -
  -
  -

Způsobů monetizace je velmi mnoho.

Monetizace výkonu počítače

- Využití CPU/GPU pro těžbu kryptoměn.
- Využití počítače pro provádění útoků na další cíle (prodej útočné kapacity).
- Využití IP adresy pro klikání na reklamy.
- Rozesílání nevyžádané pošty.

Krádež a zneužití informací

- Malware typu Banker
- Krádež a následný prodej uživatelských účtů.
- Krádež a zneužití či prodej čísel platebních karet a podobných instrumentů.
- Krádež a prodej osobních údajů (vytváření falešných identit, manipulace s jinými službami používanými uživatelem).

Monetizace

Monetizace II

- **Vydírání**
  - Malware typu Ransomware — “zaplať, nebo přijdeš o data”. Malware
  - typu Spy — “zaplať, nebo tvoje data zveřejníme”.
- **Reklama a podobné**
  - Zobrazování reklam tam, kde dříve nebyly (platba za zobrazení).
  - Zobrazování útočníkových reklam namísto původních.
  - Falešná reklama na produkty (“Váš počítač je zavirován. Kupte si náš software, ten vám ho odviruje!”).
  - Přesměrování na drahá pay-per-call telefonní čísla.

Získávání informací

Kde hledat informace, máme-li podezření, že je určitý soubor škodlivý:

- Vyhledávače na internetu — vložte jméno souboru (méně efektivní, ale občas funguje) nebo raději jeho SHA256/SHA1/MD5 hash.
- Služba **VirusTotal** (`https://www.virustotal.com`) umožňuje nahrát soubor a nechat ho zkontrolovat množstvím antivirových enginů.

  Pozor! Jde o upravené enginy proti tomu, co je součástí antivirů.

  Pozor! Obsahuje i poměrně nekvalitní enginy.

- Weby antivirových společností
- ESET Virus Radar, Kaspersky Securelist, Microsoft Malware Protection Center, atd.
- Pozor, názvy malwaru se napříč společnostmi velmi liší!