CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

# KDE VŠADE MÔŽEME NÁJSŤ MALVÉR?

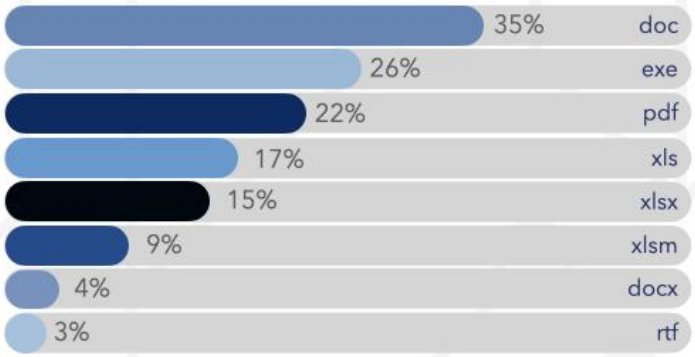
**Škodlivé súbory** sú digitálne súbory, ktoré majú za účel **poškodiť** počítačový systém, sieť alebo odcudziť údaje. Zo slova škodlivý (ang. **malicious**) je odvodené aj slovo malvér. Malvér zahŕňa širokú škálu škodlivých programov, z ktorých každý má svoj vlastný súbor funkcií a cieľov.

**Prvý** škodlivý súbor v reťazi útoku často nie je klasický spustiteľný súbor s príponou .exe, ale zvyčajne menej podozrivý typ súboru ako napríklad dokument. Ak útočník pošle priamo spustiteľný súbor, často použije trik kde dá súboru **dve prípony** (.pdf.exe, .zip.exe), čo väčšinou skombinuje aj s ikonou iného typu, prípadne len zmení ikonu a spolieha sa, že obeť si nevšimne inú príponu.

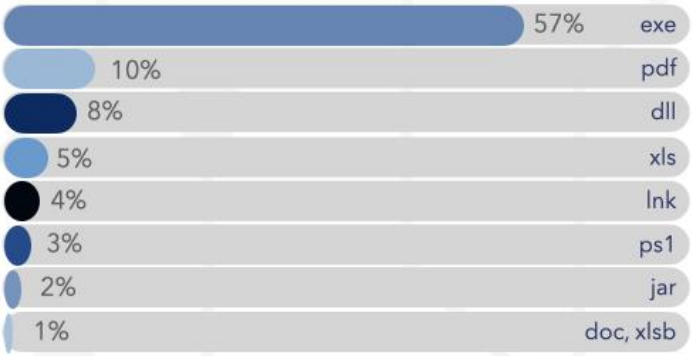
Útočník môže skúsiť zneužiť **zraniteľnosť** programu, ktorý súbor otvára a takto spustiť kód aj v dátovom súbore, ktorý nie je spustiteľný. Preto je dôležité okrem obozretnosti pri prílohách mailových správ, aj pravidelne **aktualizovať** programy, ktoré používame.

## NAJČASTEJŠIE

### TYPY ŠKODLIVÝCH SÚBOROV POSIELANÉ EMAILOM




### TYPY ŠKODLIVÝCH SÚBOROV ŠÍRENÉ NA WEBE




Zdroj: https://www.statista.com/statistics/1238996/top-malware-by-file-type/

### Microsoft Office súbory

Môžu obsahovať škodlivé **makrá**. Pri novších XML formátoch ide o **VBA** makrá, pri starších súboroch sa používajú makrá definované v **bunkách**, ktoré tiež dokážu robiť škodlivú činnosť. Škodlivé **makrá** môžu byť aj v PowerPoint súboroch a starých Rich Text Format (**.rtf**) súboroch.


### PDF súbory

Môžu obsahovať **Javascript** kód, **shellcode** ale aj priamo vložený spustiteľný **program**. Kód v **PDF** súbore často slúži ako prvý krok, ktorý sťahuje a spúšťa ďalší škodlivý program. Škodlivé **PDF** súbory vedia tiež kontaktovať vzdialené IP adresy, či spúšťať lokálne aplikácie.


### Skripty

Sú rôzneho typu - **Powershell** (.ps1), **VBScript** (.vb, .vbe, .vbs), **Python** (.py), **JavaScript** (JS), **batch** skripty (.cmd, .bat) a iné. Spustia sa, ak je na počítači prítomný tzv. prekladač na tieto typy súboru. Zvyčajne je možné skontrolovať ich obsah v textovom editore. Malvér skripty sú však zvyčajne obfuskované, teda pozmenené natoľko, že na prvý pohľad nevidíme na čo slúžia.

### Iné spustiteľné súbory

Príkladmi sú **COM** súbor (.com), **inštalátor** (.msi), Microsoft **Compiled** HTML Help (.chm), **Registration Entry** (.reg), **Screensaver** (.scr), **Java** archív (.jar) a iné. Existuje množstvo ďalších typov súborov, ktoré môžu vykonávať škodlivý kód. Ak je prípona prílohy pre nás neznáma, je potrebné si o nej zistiť viac, pred tým ako ju otvoríme.

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK