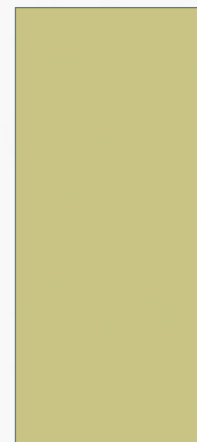


MALWARE

TOMÁŠ VIRBA, LUKÁŠ SOTÁK
2.B



ČO JE MALWARE?

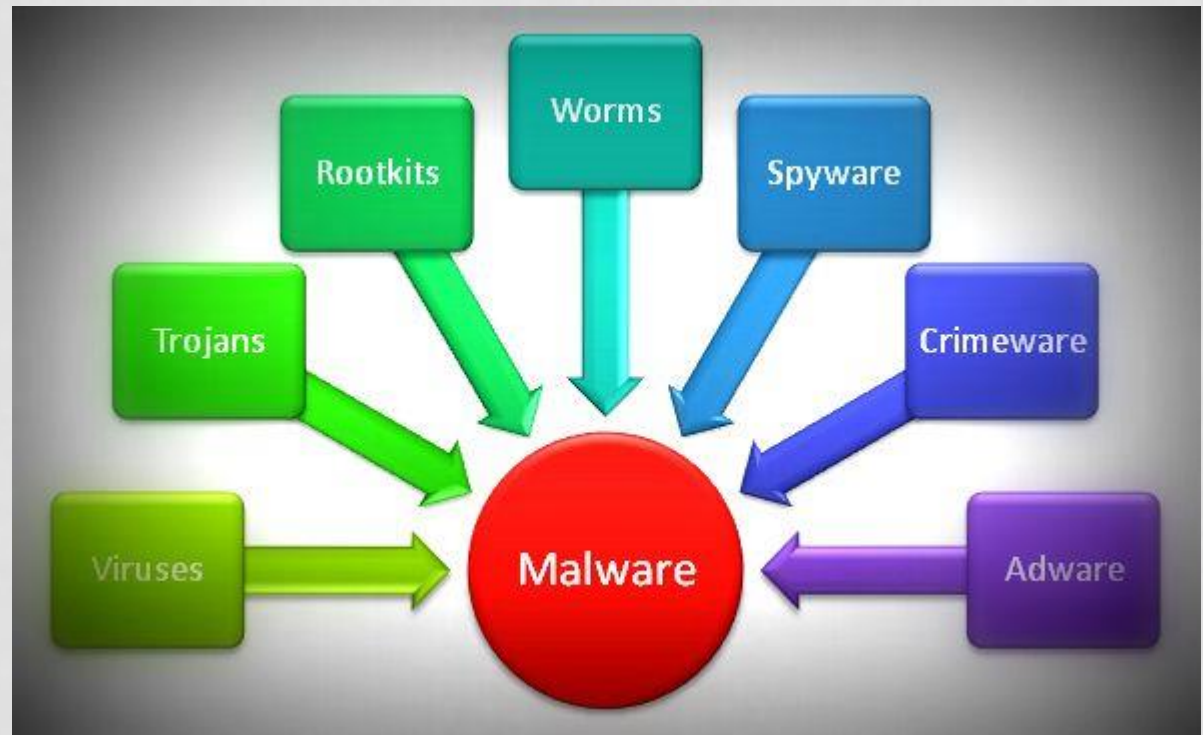
- termín malware vznikol z anglického **malicious software=škodlivý softvér**
- do kategórie malware radíme všetok škodlivý kód
- malware je akýkoľvek typ škodlivého softvéru, ktorý sa snaží infikovať počítač alebo mobilné zariadenia



0111101010101010
1010101001001000
101101001001000
0010**MALWARE**000
010100010110100
001101110101001
010010010100010

TYPY MALWARU

- Červy
- Vírusy
- SMS trojan
- Backdoor
- Spyware
- Rootkit
- Ransomware
- Botnet

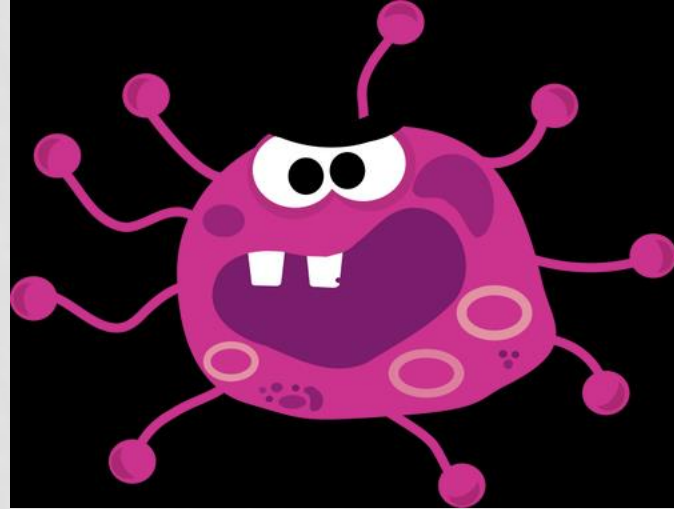


NÁKAZLIVÝ MALWARE

- **Vírus-** časť kódu, ktorý nefunguje samostatne, ale pripája sa k iným programom a rozmnožuje sa do ďalších programov
- **Červ-** samostatný program, ktorý sa rozširuje rôznymi komunikačnými kanálmi do ďalších počítačov

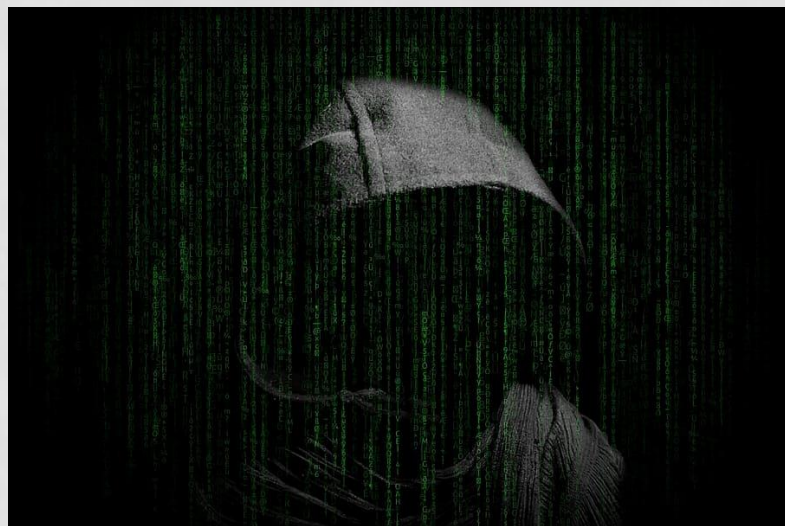
SMS TROJAN

- z nechráneného zariadenia volá alebo odosiela textové správy na prémiové telefónne čísla bez tvojho vedomia



BACKDOOR

- poskytuje útočníkovi vzdialený prístup k nechránenému prístroju bez toho, aby si o tom vedel



SPYWARE

- hľadá v tvojom prístroji e-maily, textové správy, kontakty a GPS lokalizácie
- dokáže tiež streamovať audio alebo video z kamery alebo mikrofónu nechráneného prístroja



ADWARE

- program, ktorý zobrazuje nevyžiadanú reklamu
- väčšinou nie sú priamo nebezpečné
- zvyknú byť súčasťou nejakej bezplatnej aplikácie a prinášajú takto autorovi aplikácie zisk

BOTNET

- sieť počítačov infikovaných malwarom, ktorý je riadený z nejakého centra
- počítač bez vedomia používateľa vykonáva rôzne koordinované činnosti alebo realizuje útok na niektoré služby s cieľom vyradiť ju s činnosti

ROOTKIT

- sada aplikácií, ktoré maskujú prítomnosť malwaru v počítači
- upravuje operačný systém tak, aby prítomnosť malwaru nebolo možné odhaliť bežnými prostriedkami

AKO FUNGUJE MALWARE

- autori škodlivého kódu sa väčšinou snažia útočiť z viacerých smerov (napr. cez neznáme zraniteľnosti, s použitím phishingu, skrývaním v pamäti alebo imitáciou legálnych procesov v počítači)
- dlhodobo najväčšie úspechy však útočníci oslavuje zacielených na najslabší článok reťazca, ktorým je samotný používateľ
- veľmi úspešné a lacné tak sú podvodné e-mailové kampane, ktoré útočia s pomocou techník sociálneho inžinierstva (k nakazeniu zariadenie potom stačí jedno nešťastné kliknutie)

AKO ODHALIŤ MALWARE?

- pomalý počítač je často známkou toho, že je vaše zariadenie napadnuté škodlivým softvérom
- takýto softvér môže zobrazovať vyskakovacie okná, rozosielať spam alebo spôsobovať časté pády systému
- na kontrolu, či je vaše zariadenie infikovaných, môžete použiť nástroj na vyhľadávanie malwaru, ktorý je súčasťou všetkých antimalwarových nástrojov

AKO ODSTRÁNIŤ MALWARE?

- malwaru sa najlepšie zbavíte pomocou spoľahlivého nástroja na odstraňovanie malwaru, ktorý je súčasťou každého kvalitného antimalwarového programu



AKO SA BRÁNIŤ PRED MALWARE?

- používajte účinný antivírusový a antimalwarový softvér
- neotvárajte emailové prílohy od neznámych alebo neočakávaných odosielateľov
- pravidelné aktualizácie operačného systému a používaného softvéru
- pravidelná záloha dát, najlepšie na offline úložisku



HISTÓRIA

- prvý počítačový vírus sa datuje do roku 1986, kedy bol nájdený Brain
- ten infikoval boot sektory 5.25 diskiet a v priebehu týždňov bol detekovaný po celom svete
- z počiatku išlo o pokusy jednotlivcov, ktorí skôr skúšali, čo dokážu naprogramovať, a kam až s ním môžu dostať
- primárny účel škodiť v tom poväčšine nebol
- to sa však veľmi rýchlo začalo meniť a s príchodom internetu vývoj počítačovej kriminality raketovo zrýchlil

KEDY SI DÁVAŤ OBZVLÁŠŤ POZOR

- keď sa pripájaš do nezabezpečenej Wi-Fi siete (napr. v obľúbenej kaviarni)
- pri návšteve záludných webstránok
- pri kliknutí na odkaz v e-maily alebo v chate
- pri sťahovaní aplikácií z neoficiálnych obchodov
- keď dávaš aplikácii povolenia pred inštaláciou

ZDROJE

- <http://preventista.sk/info/oplati-sa-vediet/>
- <https://www.eset.com/cz/malware/>
- <https://www.avast.com/cs-cz/c-malware>
- <https://commons.wikimedia.org/wiki/File:Tipos-de-malware.jpg>
- <https://pxhere.com/sk/photo/1566887>
- <https://www.flickr.com/photos/30478819@N08/39894487883>
- <https://www.flickr.com/photos/143601516@N03/29811036725>
- <https://freesvg.org/computer-virus-icon-vector-graphics>
- https://commons.wikimedia.org/wiki/File:Emsisoft_Anti-Malware_Logo.png
- <https://www.pexels.com/en/public-domain-photo-spuml>
- <https://www.flickr.com/photos/136770128@N07/41397208675>
- <https://www.pexels.com/sv-se/foto/cyberattack-dataintrang-datortjanst-integritet-2385332/>
- https://vzdelavanie.itakademia.sk/pluginfile.php/5066/mod_resource/content/9/M12_2_skodlivy_softver.pdf

KONIEC

