Stredná odborná škola polytechnická, Demänovská cesta 669, 031 01 Liptovský Mikuláš

Pracovný list – škodlivý kód

Predmet: informatika

Ročník: druhý, trojročný

Vytvorené dňa: 13.12.2014

Autor: Mgr. Andrej Štefaničiak

Vypracoval:

Dátum:..... Trieda:.....

Žiak:.....

Škodlivý kód (*malicious software*)

Ide o škodlivý softvér, ktorý má znepríjemňovať život užívateľovi alebo má prevziať kontrolu nad jeho počítačom. Každý škodlivý kód potrebuje pre svoju činnosť preňho známe prostredie. Rovnako ako ľudský vírus si musí nájsť tú svoju bunku, tak aj škodlivý kód si musí nájsť tú svoju časť systému, v ktorej bude uložený. Škodlivý kód sa často mylne označuje ako vírus, ktorý bol síce prvým, ale v tej dobe jediným typom škodlivého kódu. V súčasnosti však je už iba jeden z mnoho typov takýchto kódov.

Typy škodlivého kódu

Vírus je program (časť súboru), ktorý je súčasťou iného programu (súboru). Po spustení programu sa spustí aj vírus a sám sa aj replikuje (šíry).

Trójsky kôň je samostatný program, ktorý sa nevie šíriť. Môže ničiť dáta, sťahovať iné škodlivé kódy do počítača, umožniť prístup do počítača inej osobe, odosielať údaje o stlačených klávesoch (zistenie hesla...).

Boty sú programy, ktoré očakávajú príkazy od svojich tvorcov. Nakazený počítač môže byť zneužitý na rôznu činnosť bez vedomia jeho majiteľa.

Červ využíva bezpečnostné diery v programoch. Šíry sa v sieťových paketoch. Škodí tým, že inštaluje škodlivý softvér do počíta.

Spyware program, ktorý odosiela údaje o nainštalovanom softvéry, otvorených webových stránkach. Býva súčasťou bežne inštalovaného softvéru (freeware-u, sharewar-u...).

Adware je softvér, ktorý znepríjemňuje prácu otváraním nežiaducej reklamy.

Dialer je spustiteľný súbor, ktorého úlohou je zmeniť internetové pripojenie cez modem bez vedomosti užívateľa.

Hijack je škodlivý kód, ktorý mení nastavenia internetového prehliadača.

Hoax je falošná správa.

Logická bomba je programový kód, ktorý môže byť súčasťou aplikácie alebo samostatnou aplikáciou. Tento kód čaká na spustenie predvoleným sygnálom.

Pop-up okná sa objavujú po spustení aplikácie, či otvorení www stránky. Prácu znepríjemňujú zížením výkonu počítača.

Rootkit ide o program, ktorý zaistí prístupové práva administrátora. Úlohou takéhoto programu je spustiť a skryť iný škodlivý kód.

Wabbit zahlcuje systém nezmyselnými procesmi tím že sám vytvára svoje klony.

Spam je nevyžiadaná pošta, ktorá škodí svojou existenciou.

Phishing je označenie pre podvrhnuté stránky.

Ransomware je softvér, ktorý donúti užívateľa zaplatiť výkupné. Rukojemníkom sú dáta užívateľa.

Samozvaný nájomníci zneužívajú doménové názvy www stránok. Napríklad: www.google.com sa zneužije názvom www.gooogle.com.

Ochranné opatrenia pred škodlivými kódmi

Škodlivé kódy predstavujú veľkú hrozbu pre informačný systém, preto je potrebné implementovať opatrenia proti ich infiltrácii, opatrenia pre riadenie prístupov do systému a zabezpečiť primerané povedomie užívateľov. Mali by sa zvážiť

nasledovné ochranné opatrenia:

- oficiálna politika požadujúca dodržiavanie softvérových licencií a zakazujúca používanie neautorizovaného softvéru,
- formálna politika ochrany voči hrozbám spojených so získavaním súborov a softvéru cez externé siete alebo prostredníctvom iných médií,
- inštalácia a pravidelné aktualizovanie bezpečnostných záplat softvérových subaktív,
- inštalácia, pravidelné aktualizovanie a realizácia detekčných a nápravných softvérov (napr. antivírus, antispam, antispyware) na prehliadanie počítačov a externých záznamových médií,
- pravidelné vykonávanie kontrol dátového obsahu uloženého v informačnom systéme,
- plány kontinuity a obnovy činností organizácie po infekciách škodlivým kódom.

Úloha 1.

Označ správne odpovede v teste. Vždy je iba jedna odpoveď správna.

1) Čo je to škodlivý kód?
   - vírus
   - softvér
   - spam
2) Počítačové boty:
   - topánky pre počítač
   - počítače čakajúce na príkaz
   - webové stránky
3) Hoax je:
   - falošná správa
   - nevyžiadaná správa
4) Čo je to Phishing?
   - červ
   - vírus
   - podvodná stránka
5) Čo je to dialer?
   - program, ktorého úlohou je zmeniť internetové pripojenie cez modem
   - www stránka
   - pop-up okno
6) Ako škodí ransomware?
   - kradne dáta
   - ničí dáta
   - berie dáta ako rukojemníka
7) Čím škodí škodlivý kód wabbit?
   - rozosiela spam
   - zahlcuje systém nezmyselnými procesmi
   - mení nastavenia internetového prehliadača
8) Koľko typov škodlivého kódu bolo spomenutých v tomto pracovnom liste?
   - 17
   - 1
   - 11

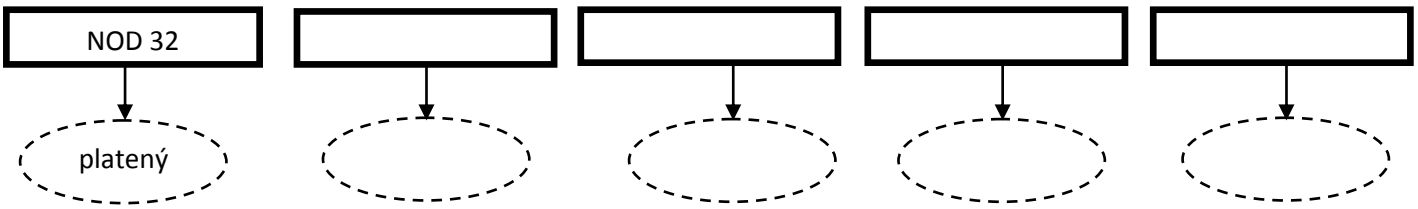
Úloha 2.

Pospájaj čiarami prislúchajúce dvojice.

phishing	program šíriaci sa v sieťových paketoch
vírus	odosiela údaje o nainštalovanom softvéry
spyware	škodlivý kód, ktorý sa dokáže šíriť sám
trójsky kôň	antivírus
adware	môže umožniť prístup do počítača inej osobe
spam	mení nastavenia internetového prehliadača
hijacker	falošná, poplašná správa
červ	podvrhnutá www stránka
nod32	znepríjemňuje prácu otváraním nežiaducej reklamy
hoax	pošta, ktorá zahlcuje poštové konto

Úloha 3.

Do prázdnych štvorčekov vpíš názvy antivírusov a do prázdnych elíps vpíš či je napísaný antivírus „zadarmo“ alebo je „platený“ (neber do úvahy úplnosť alebo neúplnosť softvéru). Ak si nevieš pomôcť, tak použi www stránky.



Ak je tento softvér je ponúknutý zadarmo, tak má vo väčšine prípadov obmädzenia.

Úloha 4.

Doplň prázdne bodkované riadky. Ak nevieš odpovedať, tak skús nájsť odpovede na www stránkach.

Aby sa mohli vírusy úspešne šíriť potrebujú sa istým spôsobom maskovať. Maskovacie techniky vírusov šíriacich sa elektronickou poštou sú:

.....

.....

Kde sa dá získať škodlivý kód trójsky kôň?

.....

Ako je možné rozpoznať phishing?

.....

.....

.....

Spameri získavajú e-mailové adresy z rôznych zdrojov, ktorými môžu byť:

.....

.....

.....

.....

Čo je to http cookies?

.....

.....

.....

.....

.....

.....

Napíš 7 názvov škodlivého softvéru.

.....

.....

.....

.....

.....

.....

.....

Kto je Miroslav Trnka? (oblasť IKT)

.....

.....

.....

.....