Microsoft

# Malware

## E o problemă de business

În medie, afacerile pierd 9,5 milioane USD pe an din cauza infracțiunilor cibernetice.[1] Este o sumă uriașă, care continuă să crească.

Infracțiunile cibernetice îmbracă mai multe forme: pierderile de date disponibilele furate, atacurile online și atacurile de tip phishing sunt printre cele mai dăunătoare pentru afaceri. Însă cele mai păguboase sunt programele **malware**.

Programele malware costă afacerile circa 5,110 USD[2] pe an, ceea ce le situează printre cele mai puțin costisitoare infracțiuni cibernetice. În schimb, ele reprezintă **cea mai frecventă infracțiune**: aproape 98%[3] dintre afaceri trec printr-un atac cu malware în fiecare an.

Atacurile cu malware sunt cele mai păguboase infracțiuni cibernetice din simplul motiv că se întâmplă tot timpul.

## Ce înseamnă malware

Malware este o abreviere pentru „malicious software", respectiv software care execută acțiuni dăunătoare pe un computer.

## Ce face un malware?

Un malware poate trimite emailuri spam de pe PC-ul tău sau să îți fure informațiile personale. Unele programe malware pot chiar să îți cripteze datele și să îți blocheze accesul la acestea, până când plătești unui hacker o răscumpărare.

Există multe tipuri diferite de malware[4], de exemplu

**viruși,**
care se răspândesc prin rețeaua ta, atașându-se la alte programe de pe PC;

**troieni,**
care arată ca un program inofensiv însă îți pot fura informațiile, dacă sunt descărcați și instalați;

**viermi,**
un tip de malware care se răspândește pe alte PC-uri prin e-mailuri, mesagerie instantanee sau partajare de fișiere.

## Cine e expus acestui risc?

**Oricine și toată lumea.**
Într-un singur an:

**20,8%**
de PC-uri din întreaga lume[5] s-au confruntat cu amenințarea malware

**175,9%**
a fost rata de multiplicare[7] medie a anumitor tipuri de malware

**36%**
dintre afacerile mici și mijlocii din Europa au suferit multiple infestări cu malware[8]

**250,000**
(și exemplare malware apărute în fiecare zi[9])

Fiecare computer conectat la internet este supus riscului de a se infesta cu malware.

## Cum au loc infestările

### E-mailurile de spam

au atașamente sau link-uri suspecte, care te păcălesc să descarci și să instalezi malware pe PC sau dispozitivul mobil.

### Programele software

de la furnizori terți pot fi infestate cu malware, care se instalează apoi pe PC-ul sau dispozitivul tău mobil.

### Unitățile portabile infestate

cum sunt unitățile flash USB pot să răspândească malware pe alte PC-uri din rețea.

### Site-uri web dăunătoare

exploatează vulnerabilitățile sistemelor tale de securitate pentru a-ți infecta PC-ul sau dispozitivul mobil cu malware.

## Majoritatea încercărilor de a infesta computerele eșuează datorită software-urilor de securitate

Chiar dacă programele malware reprezintă cea mai frecventă infracțiune cibernetică, majoritatea atacurilor de acest tip nu reușesc să infeseze computerele.

Și asta pentru că

**peste 75% dintre PC-urile din întreaga lume sunt protejate**

de software-uri de securitate în timp real, ca Microsoft Defender. [9]

Afacerile cu

**o strategie de securitate puternică, soft-uri de securitate serioase și mecanisme pentru protecția**

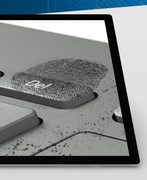
datelor, își reduc cheltuielile cauzate de infracționalitatea cibernetică cu cel puțin 2 milioane USD[10]. Te ajută și să ai un sistem eficient de backup și recuperare.

Computerele pe care nu rulează soft-uri de securitate în timp real

**pot fi de 5,6 ori mai expuse[11] la infestarea cu malware.**

## Prevenția:

cea mai bună metodă de a-ți proteja afacerea.



- **Sistemul de operare, browser-ul și celelalte programe software din firma ta sunt la zi?**
- **Faci backup la date?**
- **Angajații tăi sunt la curent cu riscurile aferente programelor malware?**
- **Ți-ai instalat un software de securitate în timp real?**

Cea mai eficientă protecție împotriva programelor malware este un produs ce oferă securitate în timp real, ca Windows Defender pentru Windows 10, Microsoft Malicious Software Removal Tool și Microsoft Antimalware pentru Azure.

1 Ponemon Institute (2016) Cost of Cyber Crime Study & Risk of Business Innovation
2 Ibid
3 Ibid
4 Definiții preluate din Microsoft Malware Protection Centre Glossary:
https://www.microsoft.com/en-us/security/portal/mmpc/shared/glossary.aspx
5 InfoSecurity Magazine (2016) Malware Infections Increase Across Multiple Sectors, Jump 50-in-1
6 Microsoft Security Intelligence Report (2015) Volume 20
7 Ibid
8 Ponemon Institute (2016) Cost of Cyber Crime Study & Risk of Business Innovation
9 Microsoft Security Intelligence Report (2015) Volume 20
10 Ponemon Institute (2016) Cost of Cyber Crime Study & Risk of Business Innovation
11 Microsoft Security Intelligence Report (2015) Volume 20