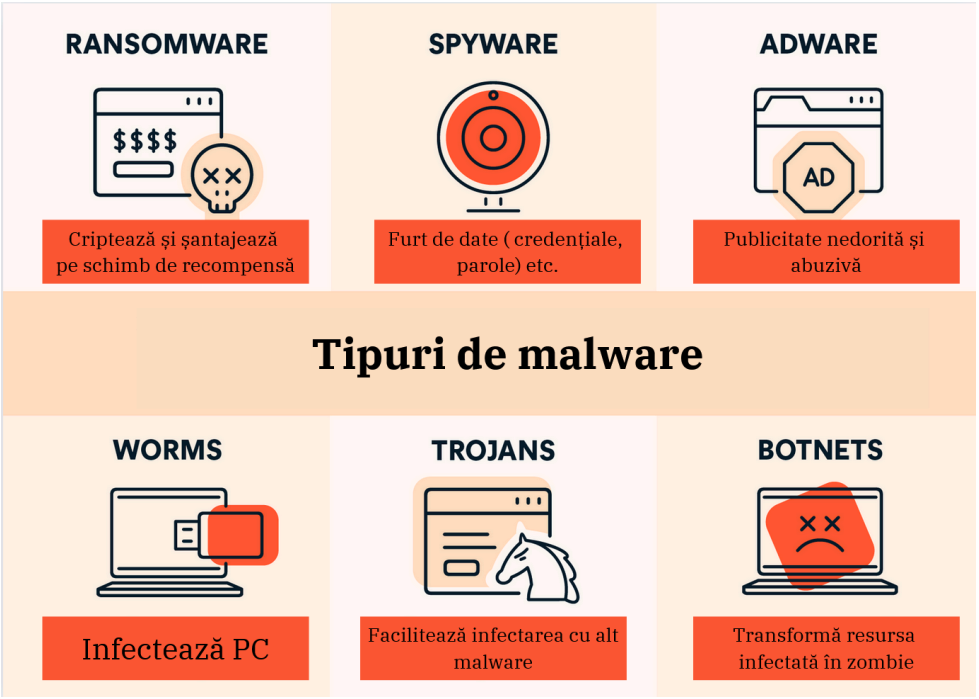
Ghid informativ privind infectarea cu malware: definiții, prevenție și răspuns la incident

Ce reprezintă un Malware

Malware-ul este un program sau cod malițios care poate provoca daune dispozitivelor dacă este executat. Unele exemple de ceea ce poate face malware-ul sunt:

- Corupe datele stocate pe dispozitivele infectate;
- Fură, șterge sau criptează datele;
- Controlează dispozitivele pentru a efectua alte acțiuni malițioase;
- Obține credențiale și accesează sistemele sau serviciile organizației tale;
- Minerit de criptomonede.



Modul de infectare sau distribuție

Malware-ul se poate răspândi prin e-mailuri de tip phishing care conțin linkuri sau atașamente malițioase. Accesarea acestor linkuri duce de obicei la descărcarea malware-ului de pe un server extern. Publicitatea malițioasă poate, de asemenea, exploata vulnerabilitățile browserului web pentru a livra și instala malware, cunoscut frecvent sub denumirea de „descărcări automate” ("drive-by downloads"). Malware-ul poate fi distribuit și prin metode precum atacuri **brute-force**, exploatarea protocolului nesecurizat de Remote Desktop (**RDP**), rețele VPN nesupravegheate și campanii de spam.

Indicatori de Infectare cu Malware

Semnele comune ale unei infecții cu malware pot include:

- Scăderea semnificativă a performanței dispozitivelor
- Utilizarea inexplicabil de mare a CPU-ului sau a discului
- Programe sau servicii necunoscute care rulează în fundal
- Comportamente inexplicabile ale dispozitivelor
- Aplicații necunoscute instalate pe dispozitive
- Activități de internet inexplicabile (rezultate de căutare suspecte, browsere care au extensii necunoscute)
- Un mesaj de răscumpărare care solicită plata pentru eliberarea fișierelor criptate.

Pentru a raporta orice incidente de securitate cibernetică, inclusiv infectarea cu malware, vă rugăm să vizitați **cyberevent.gov.md** sau să ne contactați la : **info.cert@stisc.gov.md**

Metode de prevenție

Organizațiile ar trebui să ia măsuri adecvate pentru a revizui și securiza infrastructura și sistemele lor pentru a-și spori apărarea împotriva amenințărilor malware. Următoarele măsuri pot ajuta la prevenirea infecțiilor cu malware și/sau a pierderilor financiare care pot rezulta din acestea.

Utilizați antivirus și actualizați sistemele, aplicațiile

- Instalați software antivirus/anti-malware și mențineți software-ul actualizat. Efectuați o scanare a sistemelor și rețelelor cel puțin o dată pe săptămână și scanați toate fișierele primite. Dispozitivele de stocare portabile ar trebui scanate la conectare.
- Actualizați sistemele, aplicațiile și software-ul la cea mai recentă versiune și descărcați cele mai noi patch-uri de securitate.

Activați Microsoft Office Macros doar la necesitate

Un mecanism folosit de atacatori pentru a distribui malware vine sub forma documentelor Microsoft Office malițioase care păcălesc victimele să activeze macro-comenzi pentru a vizualiza conținutul acestora. Organizațiile ar trebui să permită activarea macro-comenzilor doar atunci când este necesar.

Implementați controlul aplicațiilor

Luați în considerare instalarea software-ului de control al aplicațiilor care oferă lista albă de aplicații și/sau directoare. Listarea albă (whitelist) permite rularea doar a programelor aprobate și poate preveni rularea programelor necunoscute, cum ar fi malware-ul.

Creșterea conștientizării

Organizațiile ar trebui să desfășoare cursuri regulate de instruire pentru angajați pentru a crește conștientizarea și a învăța bune practici de igienă cibernetică, cum ar fi identificarea e-mailurilor suspecte și evitarea accesării link-urilor sau deschiderea atașamentelor din e-mailuri de la surse necunoscute sau neîncrezătoare.

Monitorizați activitățile suspecte

Fiți vigilenți în monitorizarea activităților suspecte, cum ar fi semnele indicative ale unei infecții cu malware menționate anterior]n rubrica indicatori.

Efectuați backup pentru datele critice și păstrați-le offline

Efectuați backup-uri regulate pentru a facilita restaurarea datelor în cazul unui atac de tip ransomware. Datele de backup ar trebui stocate offline și să nu fie conectate la rețea, deoarece unele variante de ransomware se pot propaga în rețea.

Pașii de răspuns la incident

Dacă organizația dvs. este victima a infectării cu malware, următorii pași vă pot ajuta în limitarea, remedierea și recuperarea sistemului:

Pasul 1: Identificarea și deconectarea dispozitivului (dispozitivelor) infectate
Identificați și deconectați dispozitivul (dispozitivele) infectat (e) imediat de la rețeaua dvs., de internet, precum și de orice dispozitive conectate prin cablu și wireless. Acest lucru va izola dispozitivul (dispozitivele) infectat (e) și va perturba capacitatea malware-ului de a se răspândi către alte dispozitive.

- Identificați dispozitivul (dispozitivele) infectat (e)
- Scoateți toate cablurile de rețea și de date și deconectați orice dispozitive conectate la dispozitivul (dispozitivele) infectat (e)
- Dezactivați conectivitatea wireless, inclusiv Wi-Fi și Bluetooth pe dispozitivul (dispozitivele) infectat (e)
- Asigurați-vă că dispozitivul (dispozitivele) infectat (e) nu poate accesa internetul.

Pasul 2: Colectați probe pentru analiză și cercetare
Utilizați un dispozitiv neafectat sau o cameră foto pentru a colecta imagini ale informațiilor importante, cum ar fi programele suspecte, orice URL-uri/linkuri și adrese de email. În plus, notați data și ora infectării, precum și descrierea despre ce făcea(dispozitivul infectat) chiar înainte de infectarea cu malware. Faceți un înregistrare a timpului când ați deconectat dispozitivul infectat, precum și orice acțiuni luate. Aceste informații pot fi importante în scopuri de investigație ulterioare.

Pasul 3: Efectuați o scanare cu antivirus
Realizați o scanare completă cu soluții antivirus pe dispozitivul (dispozitivele) infectat (e) și pe dispozitivele conectate pentru a detecta și elimina orice malware găsit. Asigurați-vă că definițiile antivirusului sunt actualizate.
Vă rugăm să țineți cont să înregistrați și/sau să luați imagini ale oricăror fișiere, programe sau alte evenimente suspecte care ar putea fi semnificative în timp ce rulați scanarea antivirusului și să înregistrați orice malware identificat înainte de a le elimina.

Pasul 4: Recuperarea și restabilirea

1. **Resetați Credențialele inclusiv Parolele -** Schimbați imediat toate parolele afectate (în special pentru conturile de administrator și alte conturi de sistem) la o parolă puternică de cel puțin 12 caractere, care include majuscule, minuscule, cifre și/sau caractere speciale. (Acest lucru va varia în conformitate cu politica de parole existentă a organizației dvs.)
2. **Asigurați-vă că malware-ul a fost eliminat-** O resetare la setările din fabrică și o instalare curată a sistemului de operare și a altor programe pot fi necesare pentru a elimina complet malware-ul de pe dispozitiv(e), deoarece există multe tipuri de malware care pot crea o formă de persistență în dispozitivul infectat. Vă recomandăm să efectuați o altă scanare completă antivirus sau anti-malware cu o definiție antivirus actualizată și să monitorizați traficul rețelei după recuperare. Aceasta este pentru a vă asigura că nu au mai rămas urme de malware în sistem.
3. **Restaurarea dintr-un backup neafectat** - Dacă aveți un backup al fișierelor originale, este posibil să restaurați fișierele din acest backup. Înainte de a începe acest proces, asigurați-vă că backup-urile sunt conectate doar la dispozitive cunoscute ca fiind curate. Scanați backup-urile pentru malware pentru a vă asigura că backup-ul nu a fost infectat.

Pașii de răspuns la incident

Pasul 5: Notificați și raportați

Dacă sunteți o organizație, notificați-vă beneficiarii, partenerii precum și personalul și angajații despre atac cât mai curând posibil, astfel încât aceștia să poată lua măsuri pentru a se proteja.

Echipa dvs. juridică vă poate asista în procesul de notificare.

- Organizațiile nu trebuie să excludă riscul de securitate informațională că datele ar fi putut fi ex filtrate dacă atacatorul a reușit să obțină acces la infrastructura sau sistemele dvs. Dacă credeți că informațiile financiare au fost compromise, contactați instituția dvs. financiară apelați 112.
- Vă rugăm să raportați în cadrul Platformei **cyberevent.gov.md** informații aferent evenimentelor sau incidentelor cibernetice. Acest lucru ne va permite să înțelegem amploarea și natura incidentului, precum și să alertăm și să asistăm o gamă mai largă de persoane și organizații.