Proiect SO Saptamana 9

În această săptămână, ne vom concentra pe analiza fișierelor dintr-un director primit ca argument în linia de comandă pentru a identifica și izola fișierele potențial periculoase sau corupte. Atacatorii utilizează mai multe tehnici, inclusiv criptarea șirurilor și apelurilor API, adăugarea de caractere aleatorii pentru a ascunde informația, includerea unor path-uri de fisiere executabile, avand denumiri explicite etc.

Pentru fiecare fișier găsit în directorul specificat care are toate drepturile lipsă, indicând astfel posibile semne de corupție sau maleficență, se va crea un proces nou care vom efectua o analiză sintactică a conținutului lui, pentru a preveni riscul de expunere la acțiuni daunatoare sistemului de operare.

Proiectul va fi structurat astfel:

- **Verificarea Drepturilor Lipse**: Se va verifica dacă fișierul respectiv are toate drepturile lipsă, iar in cazul in care acest lucru se dovedeste sa fie adevarat, se va crea un proces dedicat care va realiza printr-un script (ex: `verify_for_malicious.sh`) o analiza sintactica, pentru a determina daca este corupt sau malitios, iar mai apoi ar trebui izolat intr-un mediu separat si safe.
- **Analiză Sintactică a Fișierului**: În loc să deschidem direct fișierul, vom efectua o **analiză sintactică** a conținutului său pentru a identifica semne de maleficență sau corupție. Scriptul va include verificarea numărului de linii, cuvinte și caractere din fișier, precum și căutarea de cuvinte cheie asociate cu fișierele corupte sau malitioase, cum ar fi "corrupted", "dangerous", "risk", "attack", "malware", "malicious" sau chiar caractere non-ASCII. Daca se vor gasi una din aceste elemente, fișierul va fi considerat periculos și va fi izolat de restul fișierelor.
- **Izolarea Fișierelor Periculoase**: Fișierele identificate ca periculoase vor fi mutate într-un director special, specificat ca argument în linia de comandă, numit "izolated_space_dir". Această acțiune va preveni expunerea la potențiale amenințări și va permite investigarea ulterioară a fișierelor suspecte.

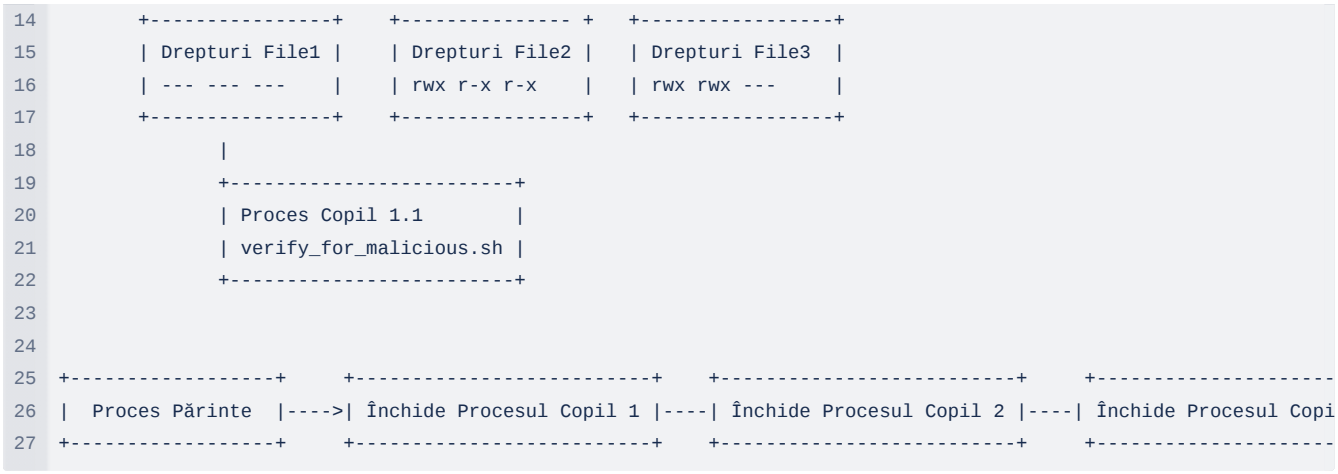
Prin aplicarea acestor măsuri, ne propunem să identificăm și să izolăm fișierele potențial periculoase sau corupte din directorul specificat, protejând astfel sistemul și datele împotriva amenințărilor de securitate.

Apelarea programului:

```
./program_exe -o director_iesire izolated_space_dir dir1 dir2 dir3
```

Exemplu de structura a directoarelor:

```
Main Directory
|_ Dir1
|  |_ File1 (Drepturi: --- --- ---)
|_ Dir2
|  |_ File2 (Drepturi: rwx r-x r-x)
|_ File4.txt
|_ Dir3
|  |_ File3 (Drepturi: rwx rwx ---)
```



- Pentru a îmbunătăți înțelegerea argumentelor de intrare ale programului, un nou indicator, "-s" (de la safe), va fi introdus ca argument în linia de comandă chiar înainte de argumentul "izolated_space_dir". Acesta va indica faptul că următorul argument este directorul desemnat pentru izolarea fișierelor potential periculoase. **Nu trebuie să existe un snapshot dedicat pentru acest director.** Programul va fi apelat:

```
./program_exe -o output_dir -s izolated_space_dir dir1 dir2 dir3
```