Analyse de Malware

IFRI Youssef et PESME Bastien

Analyse Statique

Extraction de strings

- "notepad.exe aa.txt"
- "erreur : (plus de 1 argument)"
- "usage <%s> : <%s> laphrasemagique (minuscule et chiffres | max 64 caractères)"
- "erreur : (la chaîne doit faire au maximum 64 char)"
- "usage <%s> : <%s> laphrasemagique (minuscule et chiffres | max 64 caractères)"
- "erreur : (la chaîne doit contenir uniquement les char suivants : [a-f0-9]*)"
- "usage <%s> : <%s> laphrasemagique (minuscule et chiffres | max 64 caractères)"
- "abcdefghijklmnopqrstuvwxyz0123456789"
- "%x"
- "84d" + "245" + "bd"
- "Les chaînes sont équivalentes bravo vous avez réussi le défi"
- "Les chaînes sont différentes (attention à vous)"
- "essai avec : "%s" (non fructueux)"

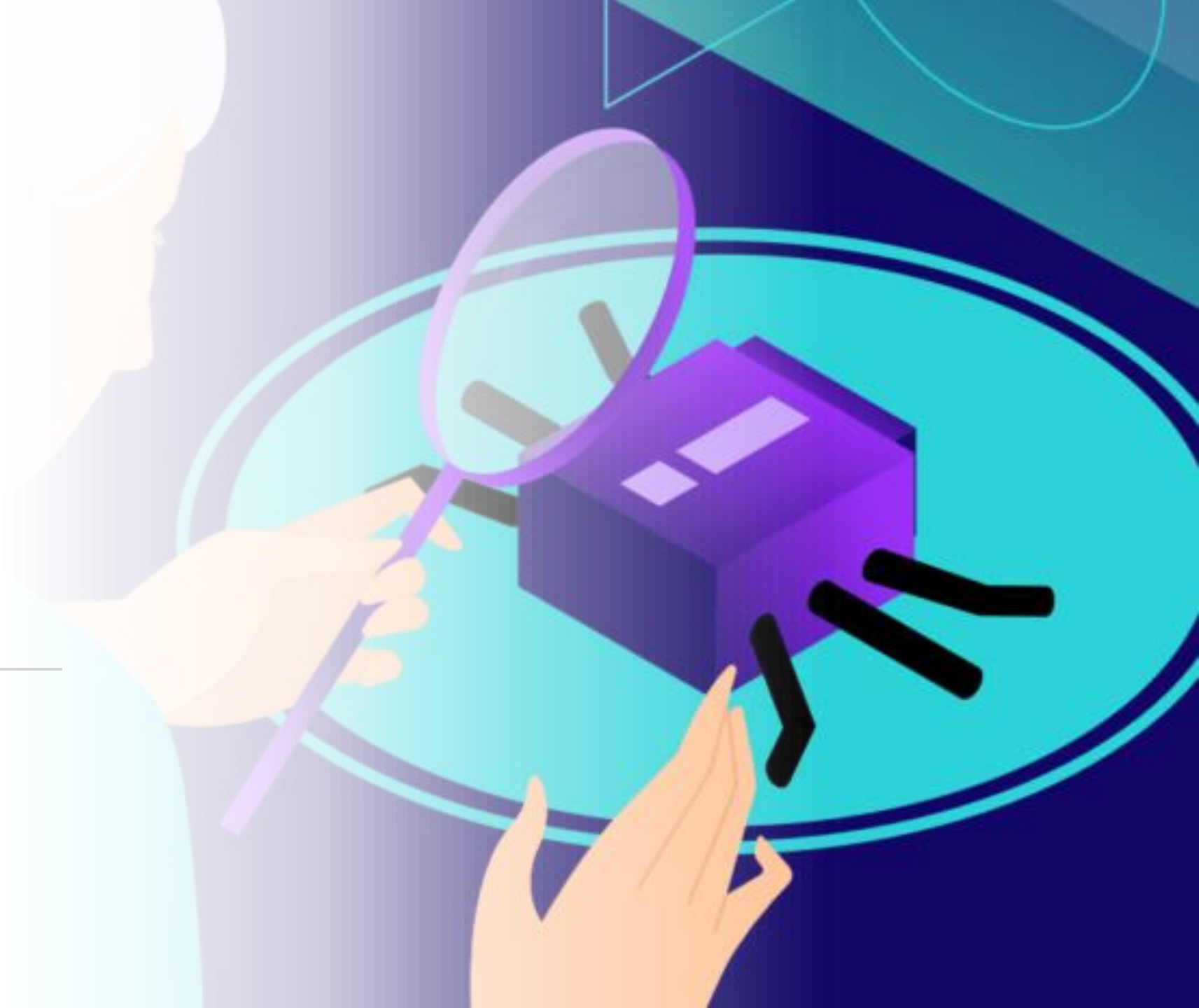
Techniques d’obfuscation

```rust
fn compute_key(input: String) -> u32 {
    let mut acc = 0u32;

    for c in input.chars() {
        (acc, _) = acc.overflowing_add(c as u32);
        (acc, _) = acc.overflowing_mul(0x401);

        let mut tmp = acc;
        tmp >>= 6;
        acc ^= tmp;
    }
```

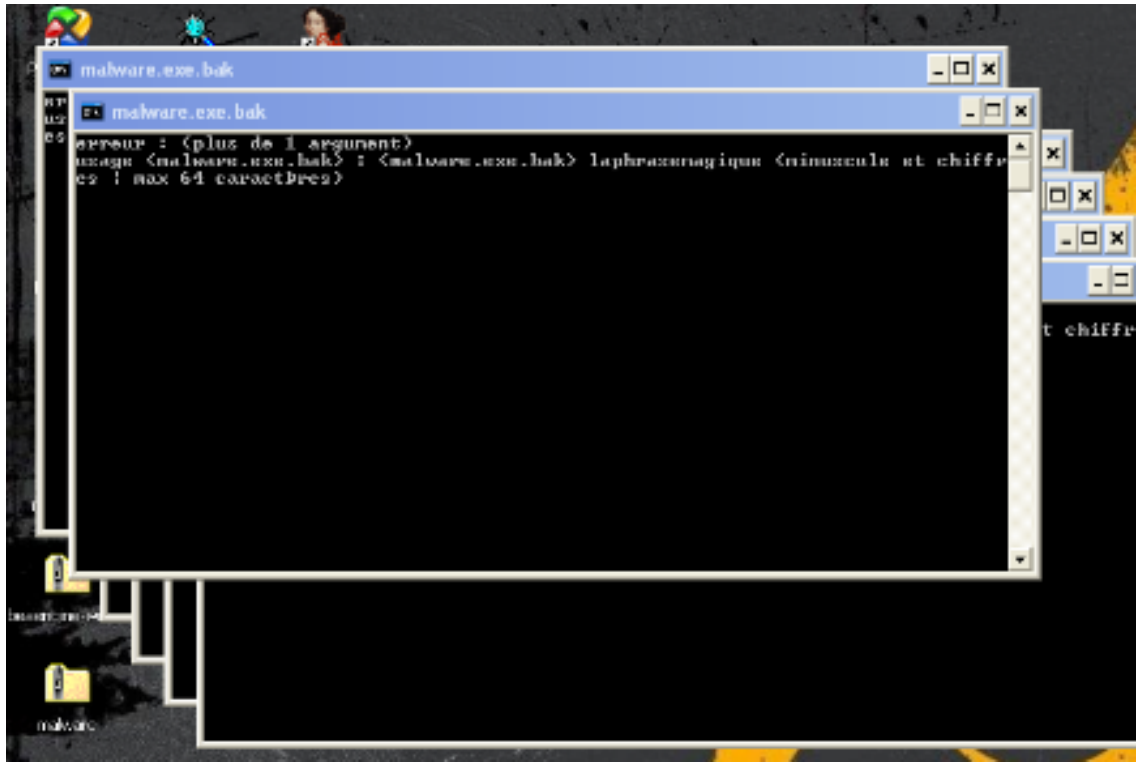
Techniques d’obfuscation

```
    let mut tmp = 8;
    (tmp, _) = acc.overflowing_mul(tmp);
    (acc, _) = acc.overflowing_add(tmp);

    let mut tmp = acc;
    tmp >>= 11;
    tmp ^= acc;
    (tmp, _) = tmp.overflowing_mul(0x8001);
    acc = tmp;

    return acc;
}
```

Analyse Dynamique



Contre-mesures



Debugage

- Contre-mesure débogage

- Fonctions:
  - Génération du haché
  - Hachage de l'entrée
  - Comparaison des deux hachés

Brute Force de la clé

Résultat

- Clé : tmmm3ri trouvée après 30 min
- 1053 clés en environ 6j de brute force
- Autres clés valides:
  - "agwequj"
  - "yve8g1l"
  - "1sw7x6l"
  - "d0bn9qx"
  - "3kop3xx"