SYNACKTIV

Rétro-ingénierie

Partie 3: Reverse Malware

Paul VIEL

Sommaire

SYNACKTIV

- Fonctionnement d'un malware
- Techniques d'anti-debug
- Anti analyse statique
- Anti analyse dynamique
- Techniques de persistance

Introduction

SYNACKTIV

- **Qu'est-ce qu'un malware ?**
- **Type de malware**
  - Backdoor / Trojan / Remote Administration Tool (RAT)
  - Ransomware / Locker
  - Stealer
  - Keylogger
  - Rootkit

Déroulement d'une infection

SYNACKTIV

- **Premier vecteur d'attaque**
  - phishing (Document piégé, URL)
  - 0Day
  - NDay
  - Social engineering (clé usb)
  - …

Vecteurs d'infection

SYNACKTIV

- Microsoft Office (Macro VBA)
- Acrobate Reader (JavaScript pour les formulaires)
- Navigateur
- Executable caché

Déroulement d'une infection

SYNACKTIV

- **Dropper**: premier programme qui récupère un second contenant la charge utile
- **Packer**: programme qui contient la charge active mais qui la cache pour contourner les détections statiques
- **Charge active**: code malveillant
- **Persistance**: techniques utilisées pour reste sur le système

Communication avec le C&C

SYNACKTIV

- Les malwares sont rarement autonomes
- Besoin de communication avec un serveur externe
  - implementation d'un kill switch
  - point faible de l'architecture

Communication avec le C&C

SYNACKTIV

- Besoin de discrétion
  - Protocole custom
  - Protocole courant: HTTP, FTP, EMAIL, DNS
  - Réseau point à point
- Besoin de robustesse:
  - C&C secondaires

Analyse de malware

SYNACKTIV

- Nécessité d'utiliser un environnement adapté
  - Execution en VM
  - Réseau séparé
- Localisation du malware
  - Faire un dump mémoire
  - Monter le disque en lecture seule
  - Dump de base de registre
  - Récupération des journaux d'évênements

Analyse automatique

SYNACKTIV

- Sandbox en ligne
  - ANY.run (https://app.any.run/)
  - Payload Security (https://www.hybrid-analysis.com)
  - Joe Sandbox (https://www.joesecurity.org/)
  - Cuckoo (https://cuckoosandbox.org/)
- Analyse d'url
  - https://urlquery.net/
- Virus Total (https://www.virustotal.com/)

Anti sandbox

SYNACKTIV

- Clefs de registre spécifiques
- Fichiers / drivers
- Temps de réponses à certains syscall
- Taille du disque dur inhabituelle
- Mouvement de souris, frappes claviers
- Wallpapers
  Example: https://github.com/a0rtega/pafish

IOC (Indicator Of Compromise)

SYNACKTIV

- Élément de forensic (« artéfact ») permettant une identification ou classification d'un code malveillant.
- Peut être sous forme d'un hash MD5, d'adresse IP, URL, nom de domaine, User-Agent HTTP, etc.
- Utilisé par les antivirus, IDS
- Règles yara et règles SIGMA

IOA (Indicator Of Attack)

SYNACKTIV

- Série d'actions qu'un adversaire doit entreprendre pour réussir son attaque.
- Toutes actions effectués par un adversaire pour préparer ses attaques.
- Tous les signaux laissés par un attaquant lors des étapes précédant une attaque.
- Utilisé par les EDR

Plateforme d'échange d'IOC

SYNACKTIV

- MISP
- https://www.misp-project.org/
- https://github.com/MISP/MISP

Anti analyse dynamique

Anti debugger

SYNACKTIV

- Linux
  - `ptrace`
- Windows
  - `IsDebuggerPresent`
  - `CheckRemoteDebuggerPresent`
  - `NTQueryInformationProcess`

Timing

SYNACKTIV

```
bool IsDebugged(DWORD64 qwNativeElapsed)
{
    ULARGE_INTEGER Start, End;
    __asm
    {
        xor  ecx, ecx
        rdtsc
        mov  Start.LowPart, eax
        mov  Start.HighPart, edx
    }
    // ... some work
    __asm
    {
        xor  ecx, ecx
        rdtsc
        mov  End.LowPart, eax
        mov  End.HighPart, edx
    }
    return (End.QuadPart - Start.QuadPart) > qwNativeElapsed;
}
```

Breakpoint

SYNACKTIV

- `INT 3` -> 0xCC : Software Breakpoint
- Vérifier s'il y en a
- En mettre partout

Autres examples

SYNACKTIV

- Casser le header ELF
- EDR
- Détection d'environnement de debug
- Liste des processus

https://evasions.checkpoint.com

Anti analyse statique

XOR des strings

SYNACKTIV

- Facile à mettre en oeuvre
- Peu de surcharge de calcul

Langage bizarre

SYNACKTIV

- Rend "moche" de décompilé IDA
- Examples:
  - AutoIT
  - Rust
  - Zig

VM

SYNACKTIV

- Grosse base de code
- Nécessite de comprendre la VM
- Example:
  - Python
  - .NET

Casser la calling convention

SYNACKTIV

```
foo:
    push RBP
    mov RDX, 0x123
    leave
    ret

main:
    call get_user_input
    mov RBX, RAX
    call foo
    cmp RDX, RBX
    jne perdu
    jmp gagne
```

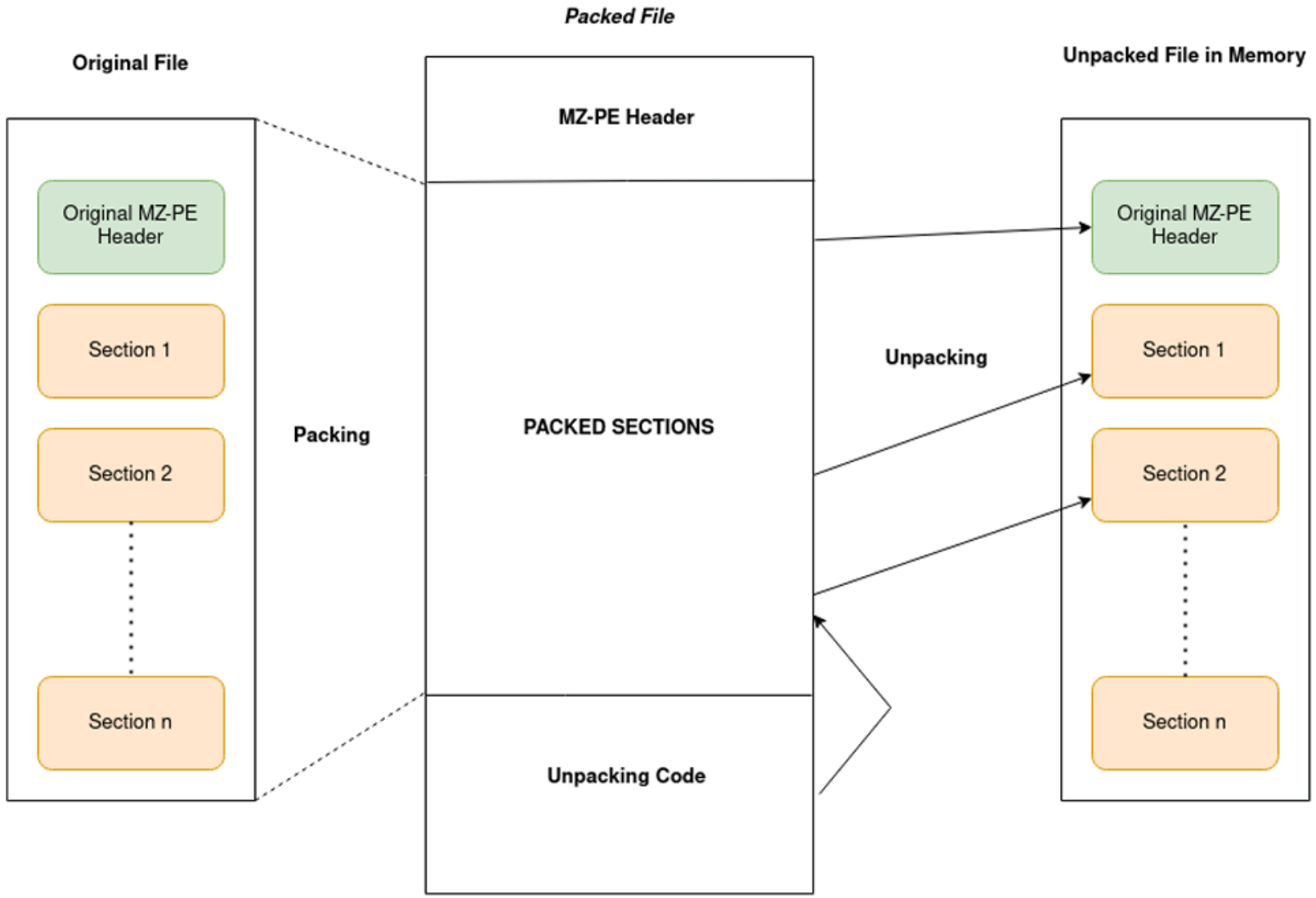
```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  __int64 user_input; // rbx
  __int64 v4; // rdx

  user_input = get_user_input(argc, argv, envp);
  foo();
  if ( v4 == user_input )
    return gagne();
  else
    return perdu();
}
```

ps: certains langages le font (Switf, go, ...)

Packer / Protector

SYNACKTIV



Autres examples

SYNACKTIV

- DeadCode
- Useless functions
- Polymorphisme
- Dynamic patching
- Control flow flattening
- Nanomite

Persistance

SYNACKTIV

- Tache planifiées
  - Linux: `cron`
  - Windows: `services`
- Driver kernel
  - Cacher des fichiers
  - Cacher des processus
- Shared Libraries
  - Linux: LD_PRELOAD
  - Windows: KnownDLLs
- Bootkit
  - MBR
  - GRUB

https://github.com/Karneades/awesome-malware-persistence

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com