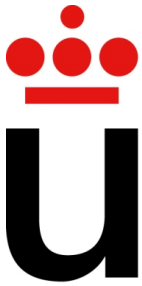


Universidad
Rey Juan Carlos

Evasión de detección en malware: implementación y análisis de técnicas de ocultación

Autor: Martín Díaz-Benito Álvarez

Tutor: Prof. Tomás Isasia Infante

14 de julio de 2025

Contenido

Motivación

- Industrialización del malware (RaaS, APTs)
- Carrera armamentística entre malware y EDR
- Objetivo principal: entender cómo se ocultan los atacantes y cómo detectarlos

Objetivos

- Estudiar técnicas estáticas y dinámicas de evasión
- Desarrollar dropper evasivo con PowerShell
- Analizar una muestra real mediante ingeniería inversa
- Evaluar resultados de detección y reflexionar sobre las técnicas de análisis

Marco teórico

- Clasificación de técnicas
  - Estáticas: ofuscación, esteganografía, empaquetamiento, criptografía
  - Dinámicas: fileless, LoTL, evasiones sandbox/debuggers
- Frameworks: Mitre ATT&CK

Metodología

- Entorno adecuado
- Desarrollo de malware en C#, metodología no iterativa al tratarse de malware
- Visibilidad en red y servidor SMB para permitir propagación durante el desarrollo
- Sandboxing y aislamiento de VMs para ejecución de malware

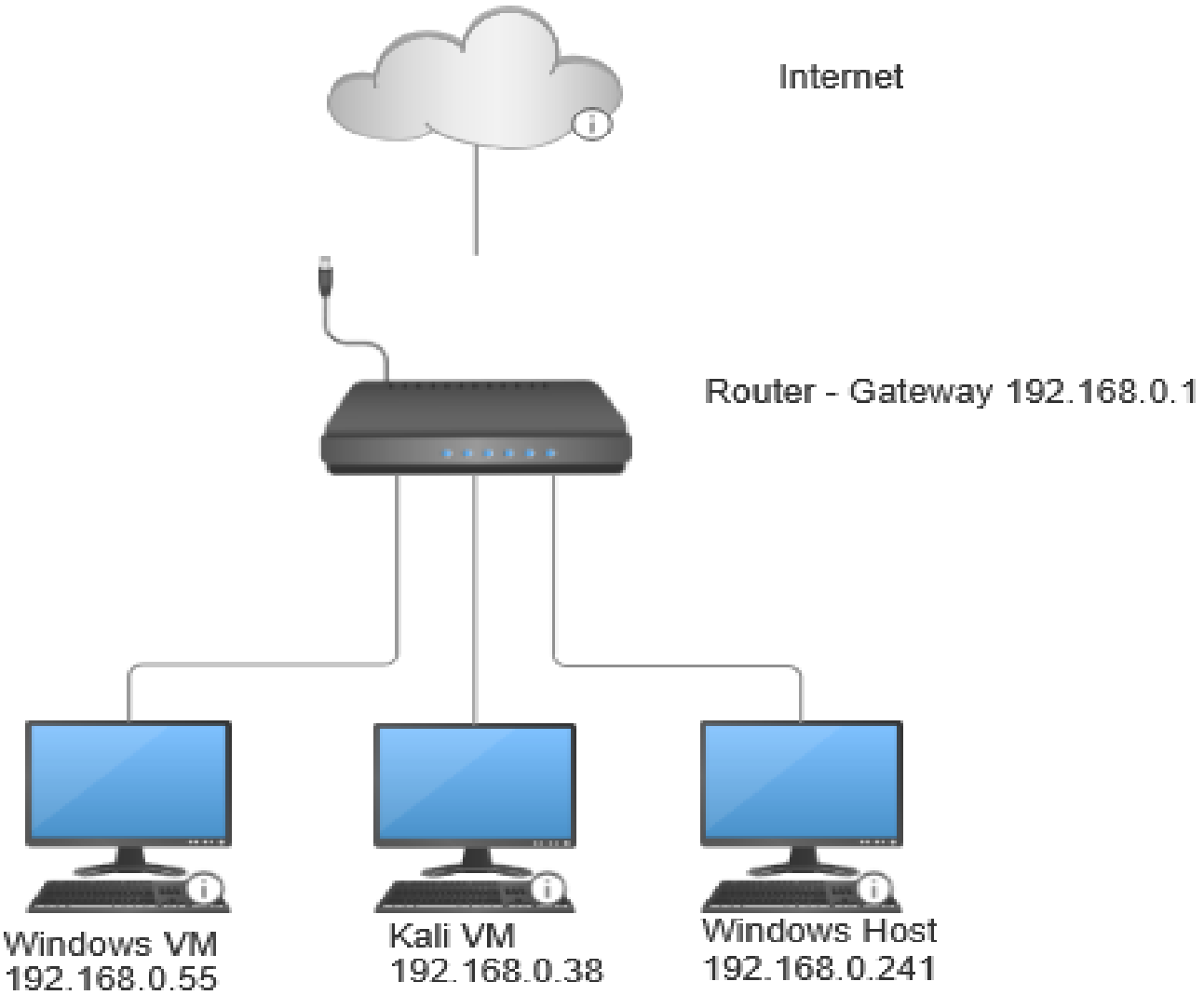
Aspectos de diseño principales del malware

- Compilado a la plataforma .NET (C#), buena integración con Windows
- Downloader con keylogger en PowerShell como payload
- Carga por reflexión + evasión de AMSI
- Enfoque fileless

Diseño de la comunicación en red

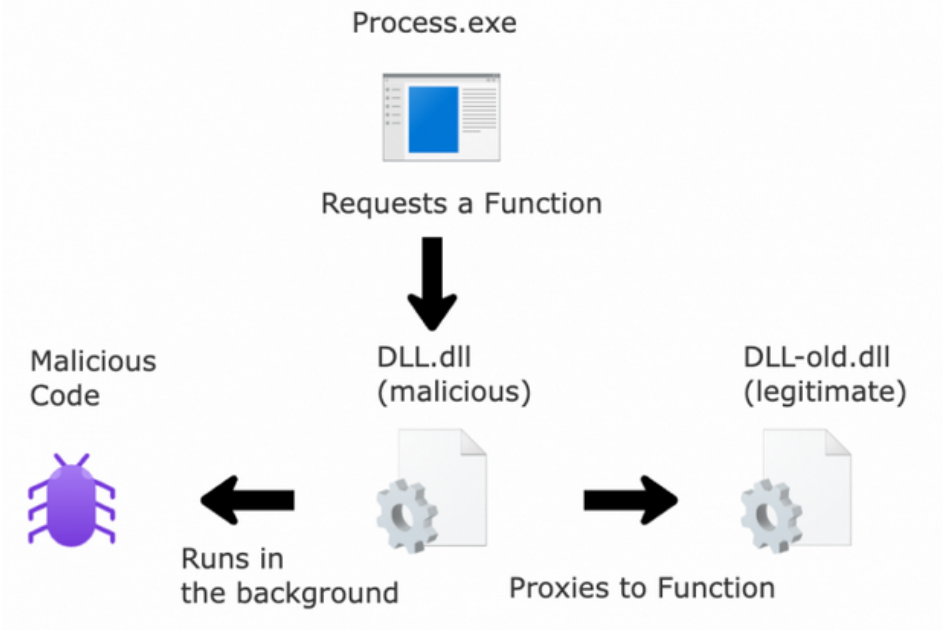
- VM Kali: Servidor C2 ligero con Flask (HTTP) y ncat (HTTPS)
- VM Windows: Victima con servidor SMB dummy
- IP Dinámica del servidor C2 desde pastebin.com
- Tráfico cifrado con HTTP/S, esteganografía y enmascaramiento de archivos

Diagrama de Red



Mecanismos de persistencia

- Tareas programadas (LoTL)
- DLL Proxying sobre 7-Zip
- Simulación de legitimidad: nombres + ubicación



Mecanismos de propagación

- SMB: escritura en recursos compartidos sin contraseña
- Discos extraíbles: replicación automática
- Ingeniería social: nombre `fileRecovery.exe`

Tráfico SMB

194	78.358291710	192.168.0.38	192.168.0.55	NBNS	104 Name query response NB 192.168.0.38
195	78.358912177	192.168.0.38	192.168.0.55	NBNS	104 Name query response NB 192.168.0.38
196	78.359188499	192.168.0.55	192.168.0.38	TCP	66 60213 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_
197	78.359250965	192.168.0.38	192.168.0.55	TCP	54 139 → 60213 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
198	78.860849799	192.168.0.55	192.168.0.38	TCP	66 [TCP Port numbers reused] 60213 → 139 [SYN] Seq=0 Win=64240 L
199	78.860952531	192.168.0.38	192.168.0.55	TCP	54 139 → 60213 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200	79.373892122	192.168.0.55	192.168.0.38	TCP	66 [TCP Port numbers reused] 60213 → 139 [SYN] Seq=0 Win=64240 L
201	79.373999991	192.168.0.38	192.168.0.55	TCP	54 139 → 60213 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
202	79.889442406	192.168.0.55	192.168.0.38	TCP	66 [TCP Port numbers reused] 60213 → 139 [SYN] Seq=0 Win=64240 L
203	79.889555863	192.168.0.38	192.168.0.55	TCP	54 139 → 60213 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
204	80.390139771	192.168.0.55	192.168.0.38	TCP	66 [TCP Port numbers reused] 60213 → 139 [SYN] Seq=0 Win=64240 L
205	80.390336493	192.168.0.38	192.168.0.55	TCP	54 139 → 60213 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206	80.391729269	192.168.0.38	192.168.0.55	BROWSER	221 Get Backup List Response
207	80.393031138	192.168.0.38	192.168.0.55	BROWSER	221 Get Backup List Response

Evasión de entornos de análisis

- Detección de VM: MACs, procesos, BIOS
- Sandboxes: ratón inactivo, `sleep`-skipping
- Debuggers: APIs, timings anómalos

Análisis de muestra real

- Muestra obtenida de theZOO, proyecto para el análisis de malware en GitHub
- AZORult: espionaje, exfiltración de credenciales
- Herramientas: IlSpy, DIE, VirusTotal, JoeSandbox
- Observaciones: inyección por reflexión con dropper personalizado, llamadas sospechosas

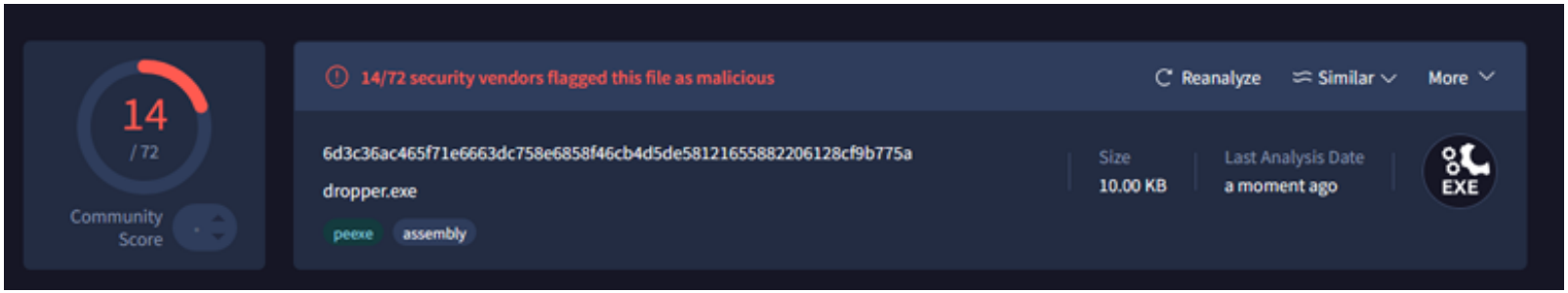
Ejecución de DetectItEasy

Resultados

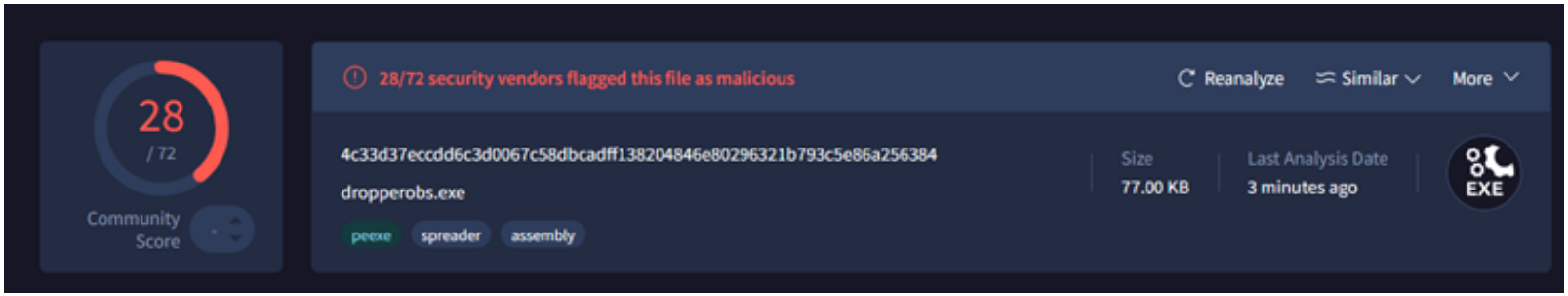
- VirusTotal: mejora significativa de detección en malware ya conocido
- La evasión en el entorno de Telefónica no tuvo éxito
- La muestra no ofuscada fue la menos detectada

Comparación de detección por muestra

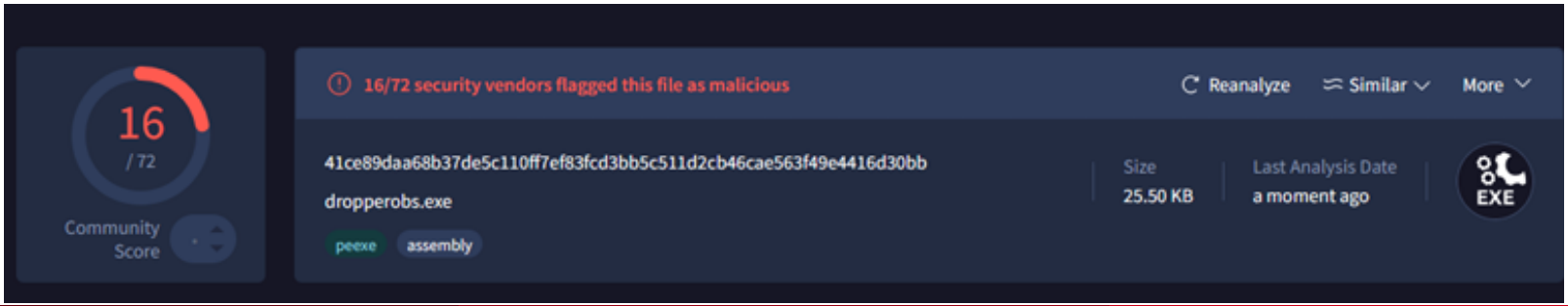
Sample 1: Original



Sample 2: ConfuserEx



Sample 3: Eazfuscator.NET



Conclusión

- Todos los objetivos del trabajo se cumplieron al menos parcialmente
- La detección por parte de los EDRs líderes y entornos corporativos presenta una dificultad significante
- Las técnicas de evasión son temporales
- EDRs necesitan combinación de técnicas de detección
- Es necesario conocer las técnicas de los atacantes para una buena detección

¿Preguntas?

¡Gracias!

¿Dudas o comentarios?