

Análisis de Malware... Sin Malware

Pedro Laguna

Consultor de seguridad

<http://www.equilibrioinestable.com>

Juan Garrido

MVP Enterprise Security

<http://windowstips.wordpress.com>







Malware

Quien está involucrado

- Creadores
- Cuerpos de seguridad
- Casas antimalware
- Usuarios finales

Información

Análisis estático

Cabeceras

Qué bibliotecas utiliza

Técnicas de evasión

Dinámico

¿Cómo se comporta en mi equipo?

¿Qué labores realiza?

Información

Actividad

¿Se encuentran activas las URL?

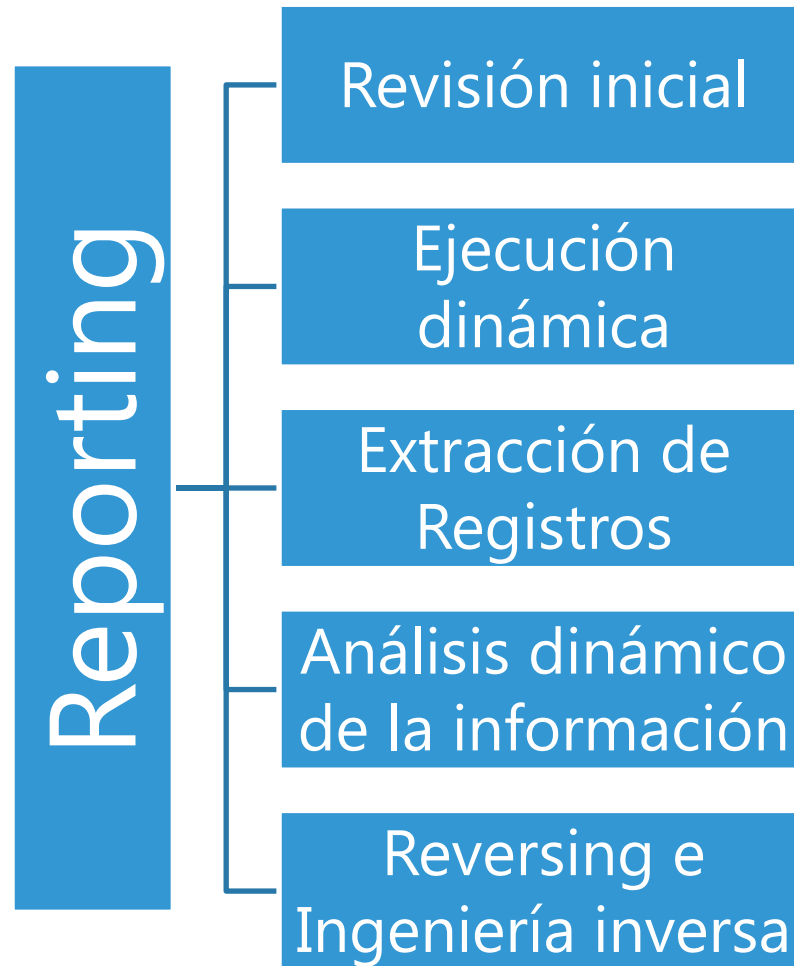
¿Se puede descargar la muestra?

Comunicación

¿Las direcciones son fiables?

¿Los dominios son confiables?

Metodología de análisis



De qué va esta charla

PERO QUÉ MIERDA ES ESTA



ANDALUZ == MENTIROSO!

CHIC@S DE LA NOCON

OS VOY A CONTAR UNA HISTORIA

InnoTec
SYSTEM

Entelgy⁷

¿Presupuesto sin compromiso?

¿Tenemos la muestra?

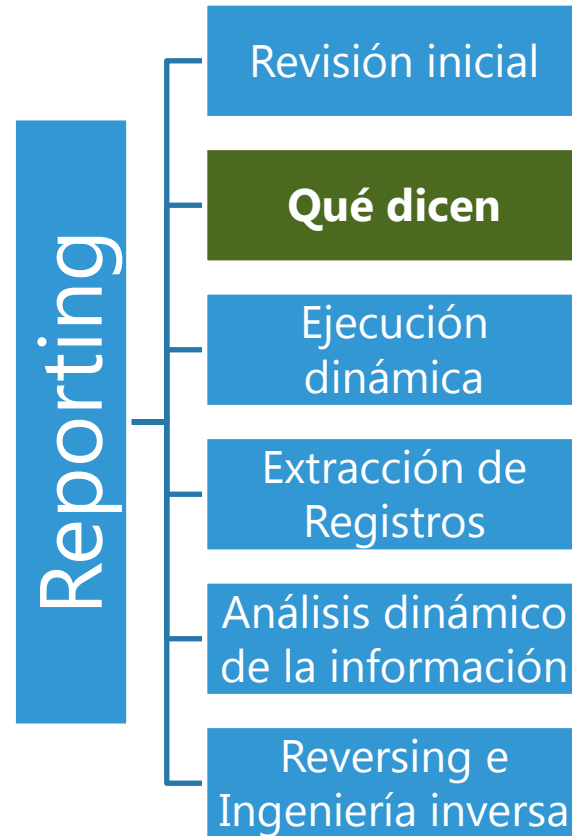
¿Sabemos realizar todas las fases?

¿Hay tiempo?

¿Se ha realizado algún trabajo ya?

¿Podemos comparar nuestro trabajo?

Metodología de análisis



TRIANA

MALWARE



CONTROL



ThreatExpert



Entelgy

Threat Intelligent Analysis

Múltiples fuentes de información

- Fuentes de Malware

- Fuentes a nivel de reputación

Comprobación de reputación

- Nivel de IP

- Nivel de dominio

- Whois (IP y dominio)

Reporting

- Informe final en DOCX



Demo



Triana en acción

Utilidades

Analistas en general

Información rápida de las principales fuentes de información

Puede abrir un primer punto de partida e investigación

Más información para un análisis e informe final

Comparar nuestro trabajo con el que se encuentra realizado

Posibilidad de encontrar la muestra activa

Una muestra == Muchas variantes

E:\Demo\027fd76caa53a2f3dbf489027f168611995e011e	Infected: VirTool:Win32/UBInject
E:\Demo\06a5fd8848d5137107a3cd8b31dedbcd4f4bfa18	Infected: VirTool:Win32/UBInject
E:\Demo\0a4379a11e3a92102df39ace5e43cd71281e3269	Infected: VirTool:Win32/UBInject
E:\Demo\0f5458b0d039b4dd4b6a1cd05da2ac6252fa73fe	Infected: VirTool:Win32/UBInject
E:\Demo\10683f690e5279cdfa25150f47833e38a422f501	Infected: VirTool:Win32/UBInject
E:\Demo\15fc0e3e6a55b4fee2e702ef9599e89f856357c2	Infected: VirTool:Win32/UBInject
E:\Demo\1732ff92f14ed8273c958e6a2bbaada7b8e07c53	Infected: VirTool:Win32/UBInject
E:\Demo\18142d7b33efbb53596544c1eae34f78d07b2588	Infected: VirTool:Win32/UBInject
E:\Demo\1c00cff9d9a4eca475389fc8cc37bd8056380de0	Infected: VirTool:Win32/UBInject
E:\Demo\258dc1ba6223c8a36b7a86087a888813e0495928	Infected: VirTool:Win32/UBInject
E:\Demo\2c939f00dba97ecf84c34a744cf66087507c85d7	Infected: VirTool:Win32/UBInject
E:\Demo\2d7hdeb96607a2527a65b18114a56823362hd633	Infected: VirTool:Win32/UBInject
E:\Demo\2fb07ef192046b0b60fc0566886997bc4f3cce64	Infected: VirTool:Win32/UBInject
E:\Demo\33cab36e18df3c2a0e008954a0faee1999e47c31	Infected: VirTool:Win32/UBInject
E:\Demo\3b8804dcbe9005ec262057e60100bb3c76365117	Infected: VirTool:Win32/UBInject
E:\Demo\3d86eace0a11f7f485a0b1d1d19c0f6a2755ceb	Infected: VirTool:Win32/UBInject
E:\Demo\4048f0d4fdf17763d71e8e5ae4e5e6c8de16c95e	Infected: VirTool:Win32/UBInject
E:\Demo\41a682a4862a252881d27e0f27a0f889341f31fb	Infected: VirTool:Win32/UBInject
E:\Demo\48203128fe0d38157c5f0de6b24d25eaa248157b	Infected: VirTool:Win32/UBInject
E:\Demo\4bbf110d358d16bcb904f7fc14d368827eaa3441	Infected: VirTool:Win32/UBInject
E:\Demo\4he41fa2fa1e1hcec9b5f74b102325d889500e02	Infected: VirTool:Win32/UBInject
E:\Demo\4c11a0322020f0bc3a100020f2f01030011003f	Infected: VirTool:Win32/UBInject

Utilidades

Multihilo

Posibilidad de analizar listas de hashes

Reducción drástica de tiempos

Útil cuando se analizan muchas muestras

Automatización total de esta fase

Conocer estado de las fuentes

Cuanta información manejan

Ratio detección antivirus



Demo



**Analizando listas de
MD5**

¿Futuro?

Soporte autenticación

Descarga de muestras

Búsquedas en sitios privados

Descarga de muestras

Almacenamiento en BBDD

Integración con Cuckoo Sandbox

Integración con HTTP Proxy

<http://windowstips.wordpress.com>

EL DIARIO DE JUANITO

Otro blog más...

stay updated via rss



LIBROS



Webcast sobre Flame o {ponga-amenaza-aquí} para administradores IT

10

Posted: junio 27, 2012 in Diario, forensics, General, Malware, Noticias, Webcast, Windows, Windows

7

Etiquetas: Flame, microsoft, sysinternals, Webcast

Hola a tod@s!

Después de todo lo que se ha hablado del infame FLAME, poco de momento se puede hablar más, hasta que no salgan nuevos hallazgos sobre el tema. Lo que si es un hecho es que parece que este Malware ha sido el nexo de unión entre piques de soluciones Antimalware. Por un lado tenemos el [post que publicó Mikko de F-Secure](#), en el que explícitamente nombra la amenaza de FLAME como una especie de LAMERADA con la originalidad de un "matón de colegio".