

Análisis de Malware

MISP y VIPER

Gerard Díaz Hoyos

KeepCoding
Bootcamp de Ciberseguridad
5a edición

MISP (Malware Information Sharing Platform):

Plataforma de intercambio de información sobre malware y amenazas.

Vamos a añadir un reporte a la base de datos de MISP (función que, cada vez más, va a ser requerida por todas las compañías que manejen cierto volumen de datos).

Usuario: alumno14@keepcoding.io

Event ID: 16

UUID: 6a9e8a0f-46cc-4c00-b2d9-57401e6c7a01

Los pasos que tendremos en cuenta serán:

1. Creación de un nuevo evento

Add Event

Date	Distribution ⓘ
<input type="text" value="2023-07-02"/>	<input type="text" value="This community only"/>
Threat Level ⓘ	Analysis ⓘ
<input type="text" value="High"/>	<input type="text" value="Completed"/>
Event Info	
<input type="text" value="TeslaCrypt analysis"/>	
Extends Event	
<input type="text" value="Event UUID or ID. Leave blank if not applicable."/>	
<input type="button" value="Submit"/>	

2. Adición de archivos relevantes

Add Attribute

Add Object

Con estos 2 botones, situados en el panel lateral, añadiremos el archivo principal del malware, los dropper, mutex, comandos relevantes, etc.

A modo de ejemplo, se visualizarían del siguiente modo:

2023-07-02	Object name: file ⓘ	Info rescale	Inherit	
2023-07-02	Payload delivery	sha1: e051cd544919980b3a96455d0e6438f2b2a0 Q		
2023-07-02	Payload delivery	filename: HELP_RESTORE_FILES.txt		
2023-07-02	Payload delivery	md5: 18b339a8e4648fa53794b7e409b614a2 Q		
2023-07-02	Payload delivery	sha256: 77d8e3ace037168599d51af446ee93c9d7458bcb1e4420eae66345f3a92af06d Q		
2023-07-02	Other	text: All your documents, photos, databases and other important files have been encrypted with strongest encryption RSA-2048 key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. If you see the main encryptor red window, examine it and follow the instructions. Otherwise, it seems that you or your antivirus deleted the encryptor program. Now you have the last chance to decrypt your files ... Show all Q		
2023-07-02	Payload installation	pattern-in-file: %COMMONPROGRAMFILES%\Microsoft Shared\HELP_RESTORE_FILES.txt		

VIPER

Plataforma para subida y descarga de archivos maliciosos de forma segura.

Usuario: alumno14

Proyecto: Ger

Tan sólo se debe subir el archivo que queramos:

Upload new Sample File

Upload Sample(s) Archive

Download Sample from URL

Download Sample from Virustotal

Choose file

118_afaba2400552c7032a5c4c6e6151df374d0e

teslacypt / practicaGerard

Upload

Samples in Project: Ger

Show 10 entries

Search:

#	SHA256	Name	Mime Type	Size	Tags
No data available in table					

Showing 0 to 0 of 0 entries

First

Previous

Next

Last

Y ya estará disponible para la descarga:

Home / Ger / 4f9d3da9e6a8f8c53683744ba76d359d897739e5c6f0d4263c2b3b8acc6abaab

Sample Info

Notes

Modules

Hex View

118_afaba2400552c7032a5c4c6e6151df374d0e98dc67204066281e30e6699dbd18.zip

Download

Delete

Meta	File ID	1
	Uploaded	Mon, 5 Jun 2023 06:01:29 +0000
File Info	Name	118_afaba2400552c7032a5c4c6e6151df374d0e98dc67204066281e30e6699dbd18.zip
	Size	169.4 KB (173514 bytes)
	Type	Zip archive data, at least v6.3 to extract, compression method=AES Encrypted
	Mime	application/zip
Hashes	MD5	d5256366060402d3deec688417dcca4
	SHA1	acc13a83f7a58fcc78019fea5c89262a62e45855
	SHA256	4f9d3da9e6a8f8c53683744ba76d359d897739e5c6f0d4263c2b3b8acc6abaab
	SHA512	6bdc022f905a730b7bcd8e1e0706a61ce664608cc2634cd4e07dcb5f08636d275cfab9f631ab59227bac93335bddf43b57fbfd11fea7e0ba59603ff9d45152eff
	CRC32	4BF128A5