ANALISIS MALWARE



ÍNDICE

1. MISP

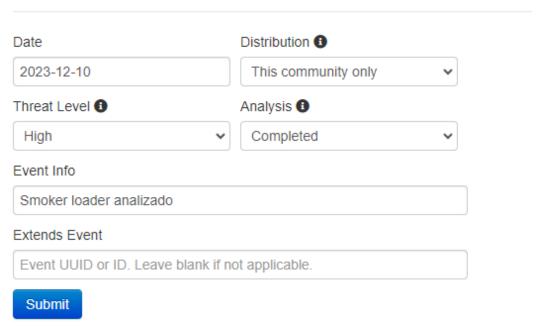
- 1.1 añadimos el evento
- 1.2 Añadimos los objetos
- 1.3 Añadimos Atributos
- 1.4 Añadimos IPS
- 1.5 Añadimos Procesos
- 1.6 Añadimos persistencia
- 1.7 Añadimos Attack pattern

1.MISP

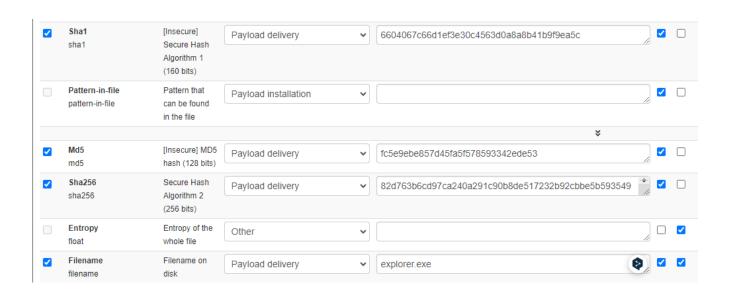
Usuario: Alumno11@keepcoding.io

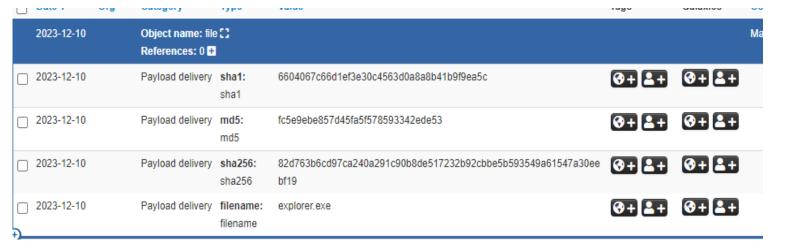
1.1 añadimos el evento

Add Event



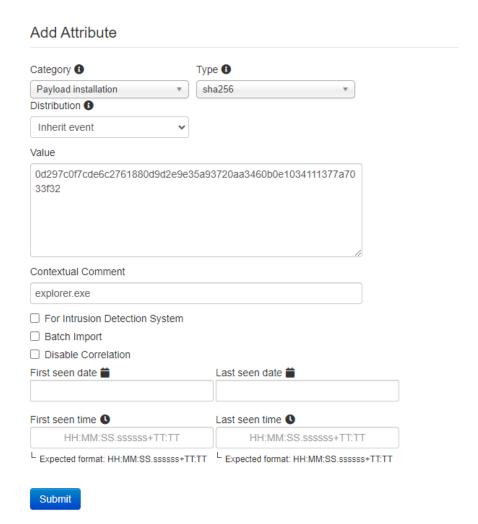
1.2 Añadimos los objetos





Objeto creado.

1.3 Añadimos Atributos



□ Date: O	iy c	Jalegory	туре	value	iays	Galaxies	Comment	Correlate	Events	reeu mis	IDS	DISTIDUTION
2023-12-10	F	Payload delivery	sha256	12cbb662f357a3be5dac4e19a58c7079cfc6c180fff52db827640f1a3b74c75 d	⊗ + ≜ +	3 + 2 +	B7C1.exe		17 18		~	Inherit
2023-12-10	F	Payload delivery	sha256	f3951f0fe95de7deaddae4c07656dfb39ebc46fca7bb07bdf711a886f33d8b8 6	⊗ + ≗ +	⊗ + ≗ +	WerFault.exe				~	Inherit
2023-12-10	F	Payload delivery	sha256	015e3f63a4b336ac9dbfa5304eaf2954277a5d2501d52f5b8b67767c96e8df 2c	⊗ + ≜ +	3 + 2 +	288D.exe		17 18		~	Inherit
2023-12-10	F	Payload delivery	sha256	93b169fd78f865f3ecd315d176947d8bc5c45794d0334c365818f058e4645c 9a	⊗+ ≗ +	3+2+	AppLaunch.exe				~	Inherit
2023-12-10	F	Payload delivery	sha256	e62f2be0a979e6d7d633ac099e2ce579e3a0b02799c0cbec91cb64e41a020 364	⊗ + ≜ +	⊗ + ≜ +	regsvr32.exe	V			~	Inherit
2023-12-10	F	Payload delivery	sha256	c7267b7f6d9fe20ab12cc545ad77627e3a37f86a94bca3284693677a7152f6b2	⊗ + ≜ +	⊗+≜ +	tasklist.exe					Inherit
2023-12-10	F	Payload delivery	sha256	24f8ba2105b5be091540c801d4ce6471b5d2f28479dc3905c0d1236c5f858 82b	0 + 2 +	⊗ + ≜ +	cmd.exe					Inherit
2023-12-10	F	Payload delivery	sha256	2df7ac59e0436af254bd931c9bf49ca3a21a43ed4087cadf8ccc7b4ca40aa9 53	⊗ + ≜ +	3+2+	findstr.exe				~	Inherit
2023-12-10	F	Payload delivery	sha256	c35f6c7b6388fe6a45a6b5680b133ccc54a3c57b6c0d8a1d9b40359f2c7154 07	⊗ + ≗ +	3+ +	WerFault.exe				~	Inherit
2023-12-10	F	Payload delivery	sha256	8a02bc37c96f772bf549b576f3d47d399c6d4df018d57dfb94c145a076889b 6f	Ø + 2 +	0 + 2 +	PING.EXE				~	Inherit
2023-12-10	F	Payload installation	sha256	0d297c0f7cde6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f 32d	0 + 2 +	0 + 2 +	explorer.exe				~	Inherit

Atributos añadidos.

1.4 Añadimos IPS

Network activity	ip-src	179.25.46.206	0 + 2 +	3 + 4 +	V		~	Inherit
Network activity	ip-src	34.143.166.163	0+4 +	⊗ + 2 +	V	16 17	~	Inherit
Network activity	ip-src	91.215.85.1	3+2+	⊗+2 +	V		✓	Inherit
Network activity	ip-src	181.168.176.36	⊗ + ≗ +	⊗+2 +	V		Z	Inherit
Network activity	ip-src	172.67.137.48	3 + 4 +	⊗ + ♣+	✓		✓	Inherit

Ips añadidas.

1.5 Añadimos Procesos

Payload delivery	text	Se están utilizando estas herramientas para listar procesos y buscar cierto s procesos en la lista, como "avastui exe", "avgui.exe", "nswscsvc.exe", "so phoshealth.exe", "wrsa.exe", entre otros.	0+	0 + 2 +	tasklist.exe y findstr.exe	✓	Inherit
Payload delivery	text	Un proceso de alojamiento de tareas de Windows.	0+	⊗ + ≜ +	taskhost.exe (PID 1896)	✓	Inherit
Payload delivery	text	Un proceso relacionado con la instrumentación de administración de Windows.	0+	8+4 +	WmiPrvSE.exe (PID 5188)	✓	Inherit
Payload delivery	text	Varias instancias de "svchost.exe" están ejecutándose. Este es un proceso legítimo de Windows que aloja servicios del sistema.	0+	Ø+ & +	svchost.exe	✓	Inherit
Payload delivery	text	Un proceso legítimo de Windows que gestiona las credenciales de inicio d e sesión.	0+	0 + 2 +	Isass.exe (PID 1884)	✓	Inherit

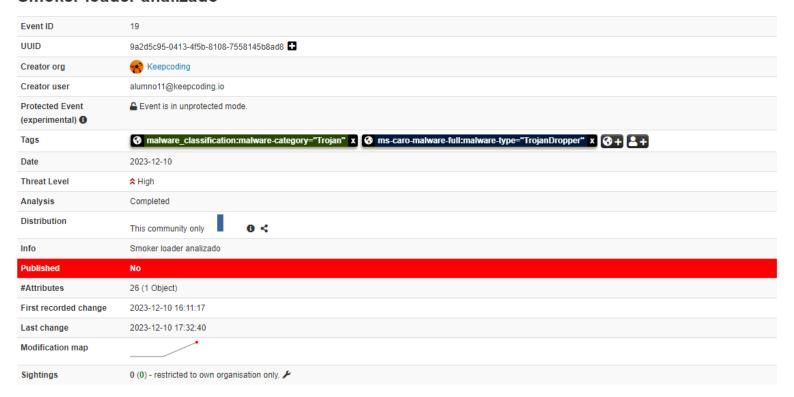
1.6 Añadimos Persistencia

□ Date ↑	Org	Category	Туре	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
2023-12-10		Persistence mechanism	text	Se están utilizando dos instancias de "regsvr32 exe" para registrar un archi vo DLL ubicado en la carpeta temporal del usuario "%TEMP%1942B dll". E sto podría ser una técnica utilizada por malware para persistencia o ejecuc ión de código malicioso.	0+2+	0+2+	regsvr32.exe (PID 4008 y PID 2804	V			✓	Inherit

1.7 Añadimos Attack pattern



Smoker loader analizado



Evento id:19

https://13.48.162.234/events/view/19