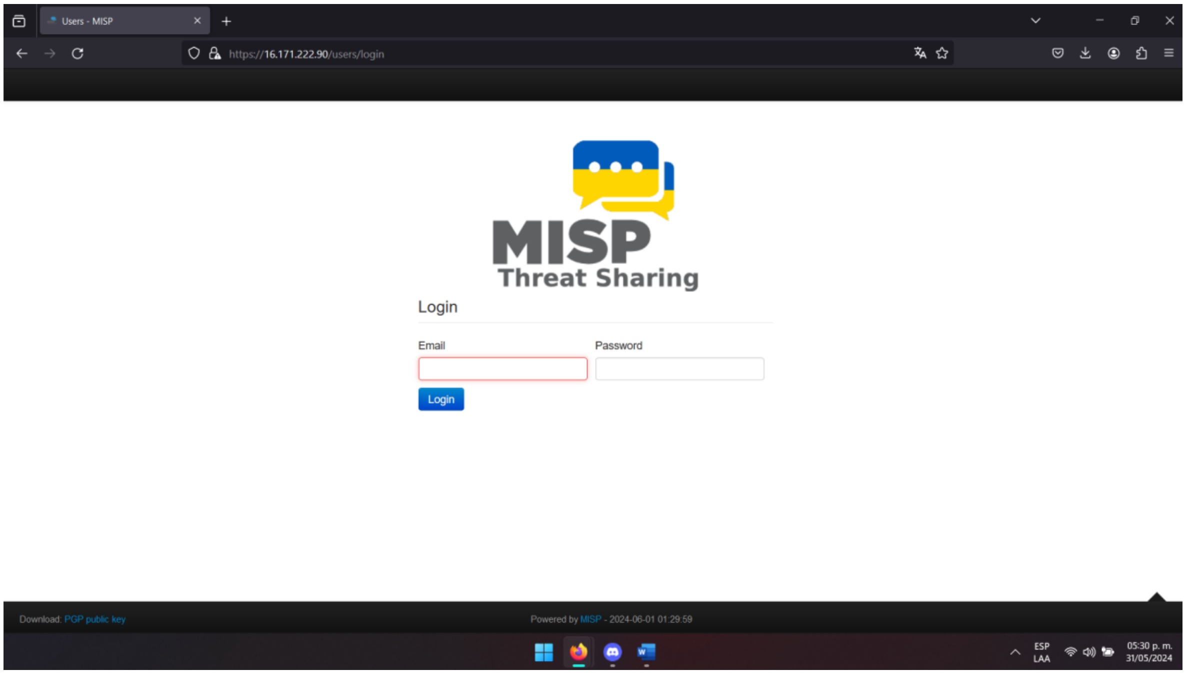
Registro en MISP

Event ID: 14

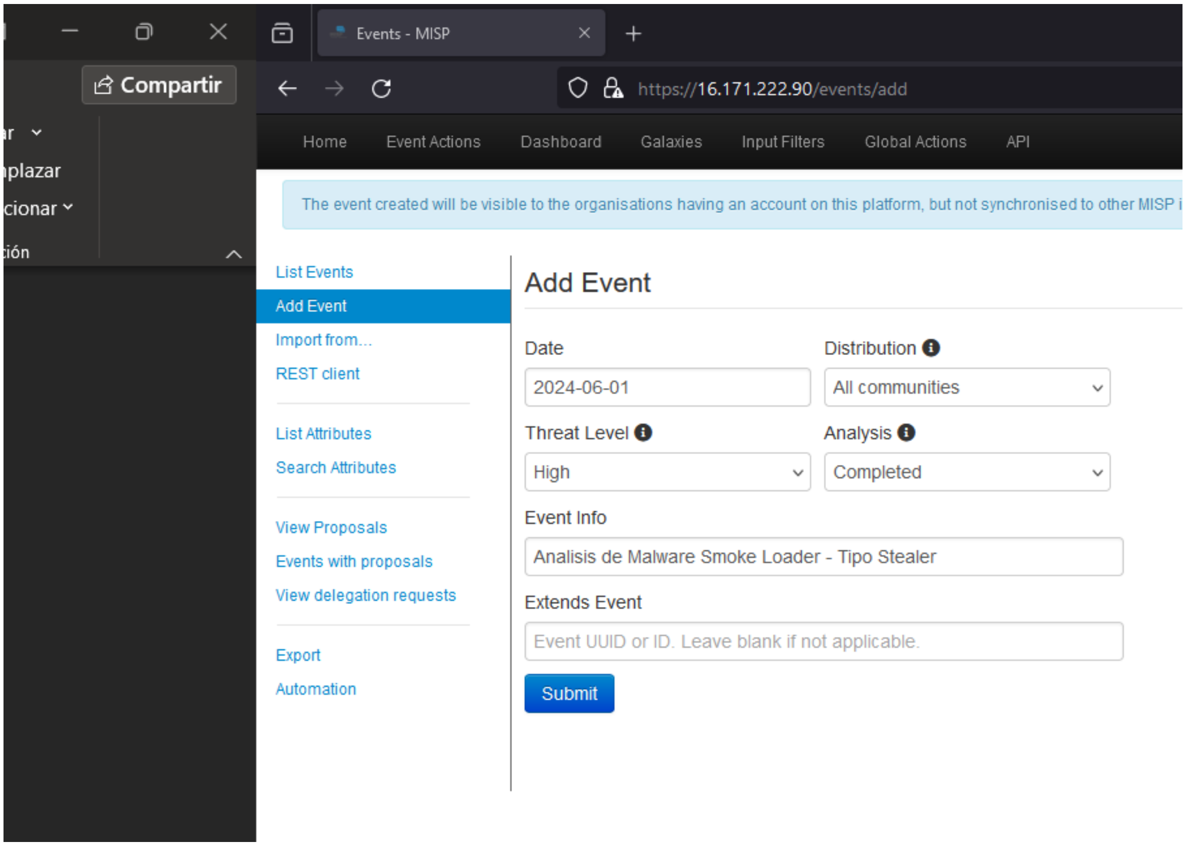
UUID: bfb2a40c-747f-4d2f-a547-507d3b27260c



https://16.171.222.90/users/login

Download: PGP public key

Powered by MISP - 2024-06-01 01:29:59



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP i

Add Event

Date: 2024-06-01

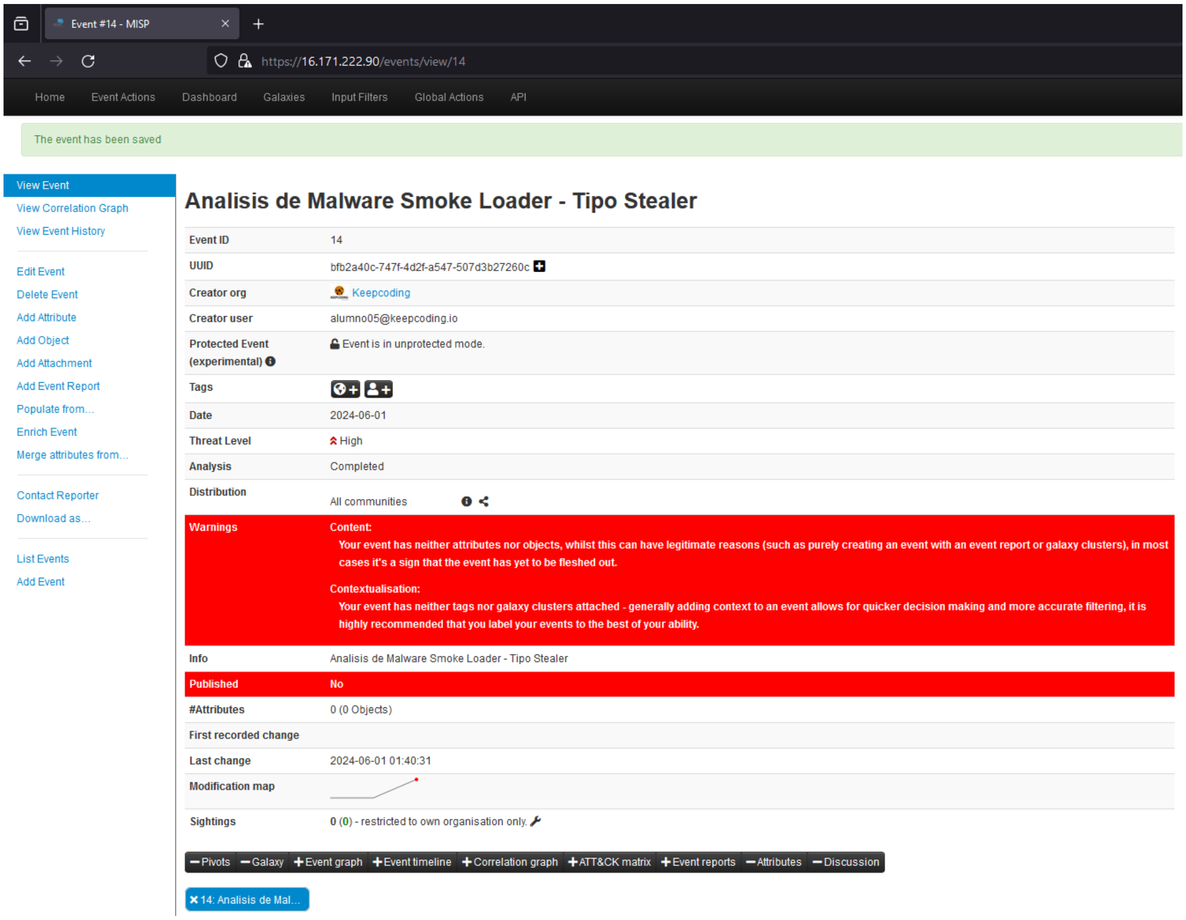
Distribution: All communities

Threat Level: High

Analysis: Completed

Event Info: Analisis de Malware Smoke Loader - Tipo Stealer

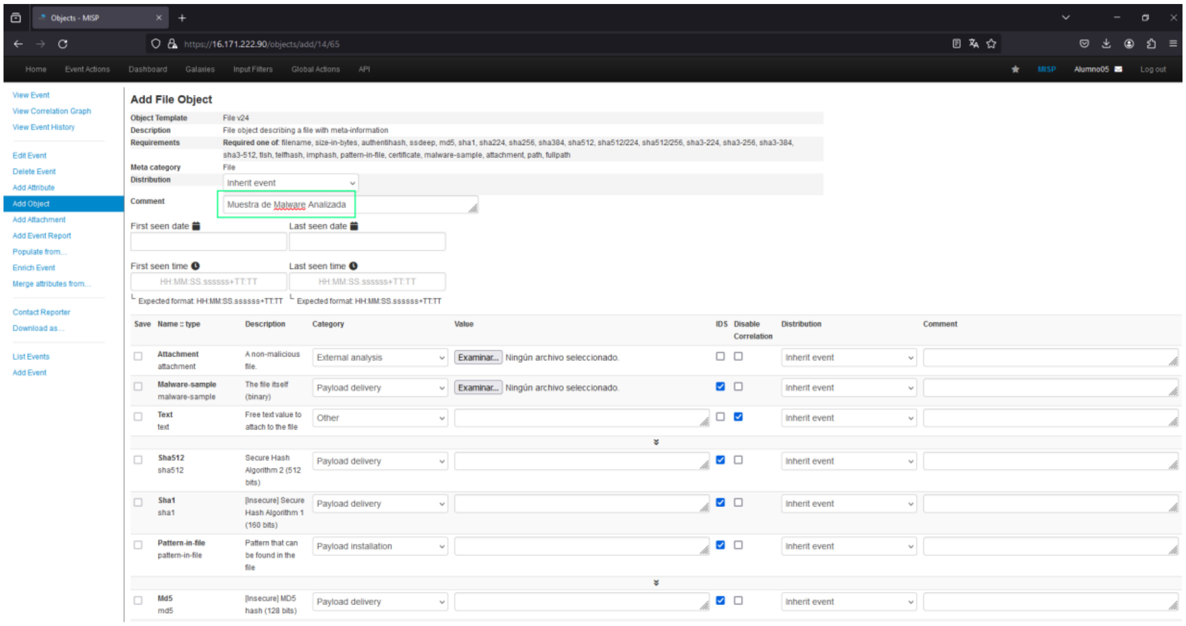
Extends Event: Event UUID or ID. Leave blank if not applicable.



The event has been saved

Analisis de Malware Smoke Loader - Tipo Stealer

Event ID	14
UUID	bfb2a40c-747f-4d2f-a547-507d3b27260c
Creator org	Keepcoding
Creator user	alumno05@keepcoding.io
Protected Event (experimental)	Event is in unprotected mode.
Tags	
Date	2024-06-01
Threat Level	High
Analysis	Completed
Distribution	All communities
Warnings	**Content:** Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out. **Contextualisation:** Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.
Info	Analisis de Malware Smoke Loader - Tipo Stealer
Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2024-06-01 01:40:31
Modification map	
Sightings	0 (0) - restricted to own organisation only.



Add File Object

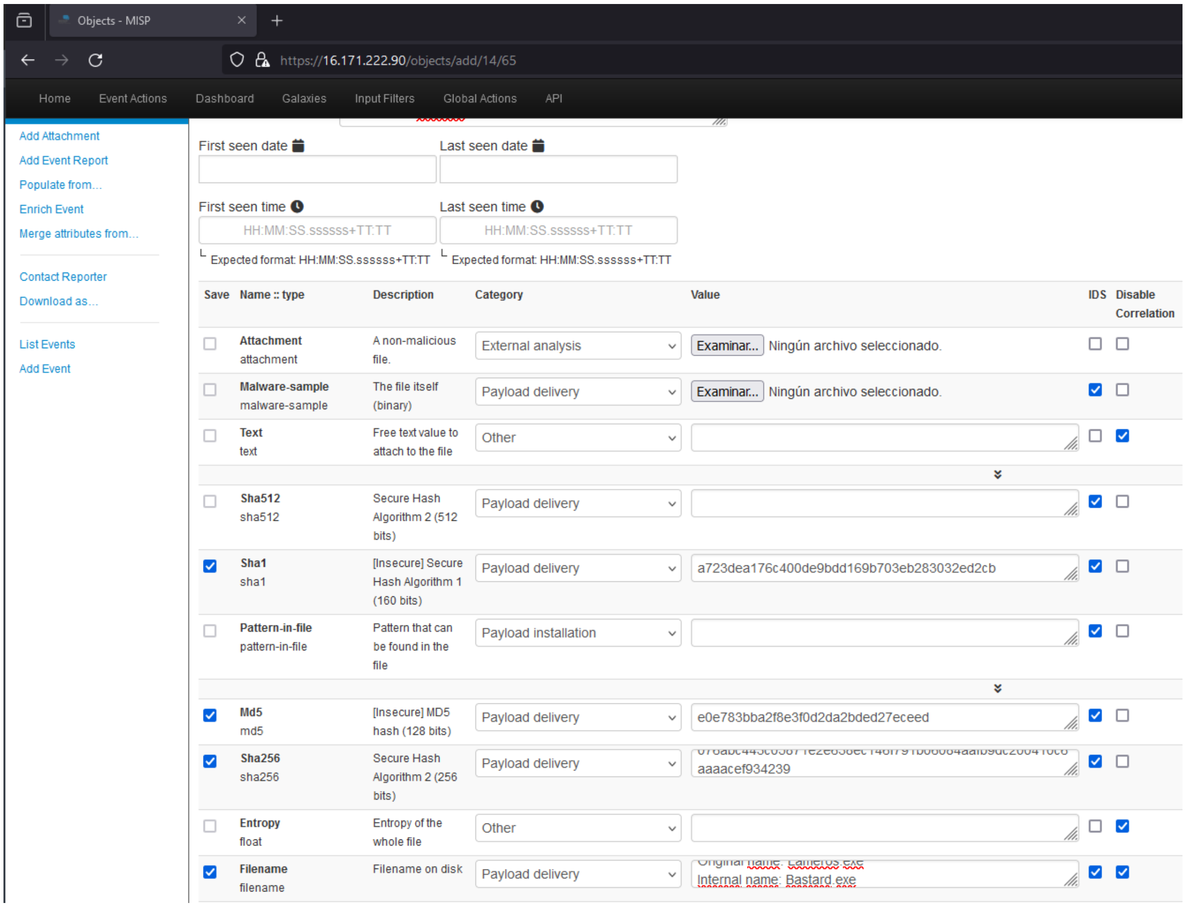
Object Template	File v24
Description	File object describing a file with meta-information
Requirements	**Required one of:** filename, size-in-bytes, authentihash, ssdeep, md5, sha1, sha224, sha256, sha384, sha512, sha512/224, sha512/256, sha3-224, sha3-256, sha3-384, sha3-512, tlsh, telfhash, imphash, pattern-in-file, certificate, malware-sample, attachment, path, fullpath
Meta category	File
Distribution	Inherit event
Comment	Muestra de Malware Analizada

First seen date:
Last seen date:

First seen time: HH:MM:SS.ssssss+TT:TT
Last seen time: HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT

Save	Name :: type	Description	Category	Value	IDS	Disable Correlation	Distribution	Comment
□	**Attachment** attachment	A non-malicious file.	External analysis	Examinar... Ningún archivo seleccionado.	□	□	Inherit event	
□	**Malware-sample** malware-sample	The file itself (binary)	Payload delivery	Examinar... Ningún archivo seleccionado.	☑	□	Inherit event	
□	**Text** text	Free text value to attach to the file	Other		□	☑	Inherit event	
□	**Sha512** sha512	Secure Hash Algorithm 2 (512 bits)	Payload delivery		☑	□	Inherit event	
□	**Sha1** sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	Payload delivery		☑	□	Inherit event	
□	**Pattern-in-file** pattern-in-file	Pattern that can be found in the file	Payload installation		☑	□	Inherit event	
□	**Md5** md5	[Insecure] MD5 hash (128 bits)	Payload delivery		☑	□	Inherit event	



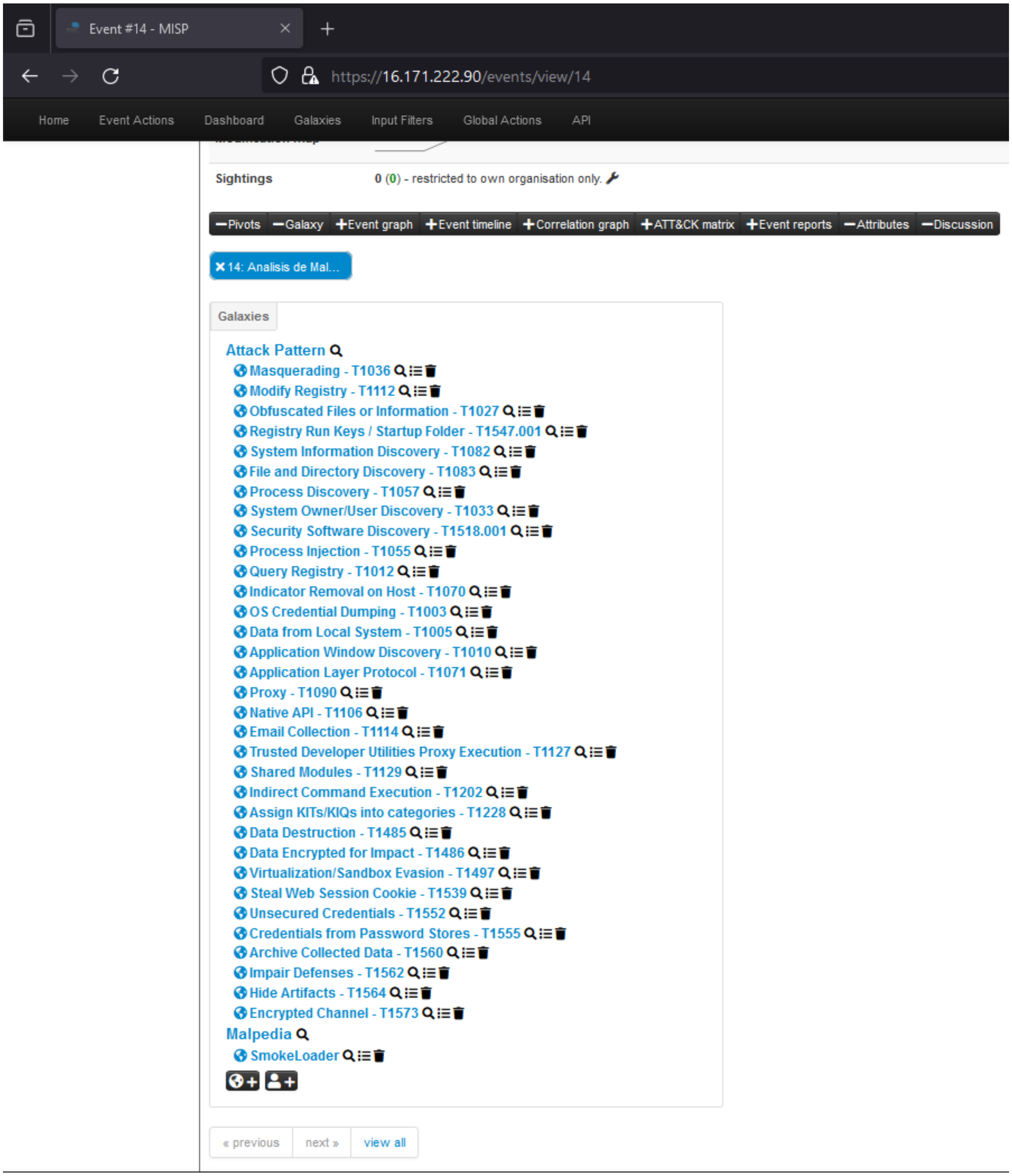
First seen date

Last seen date

First seen time: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT

Last seen time: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT

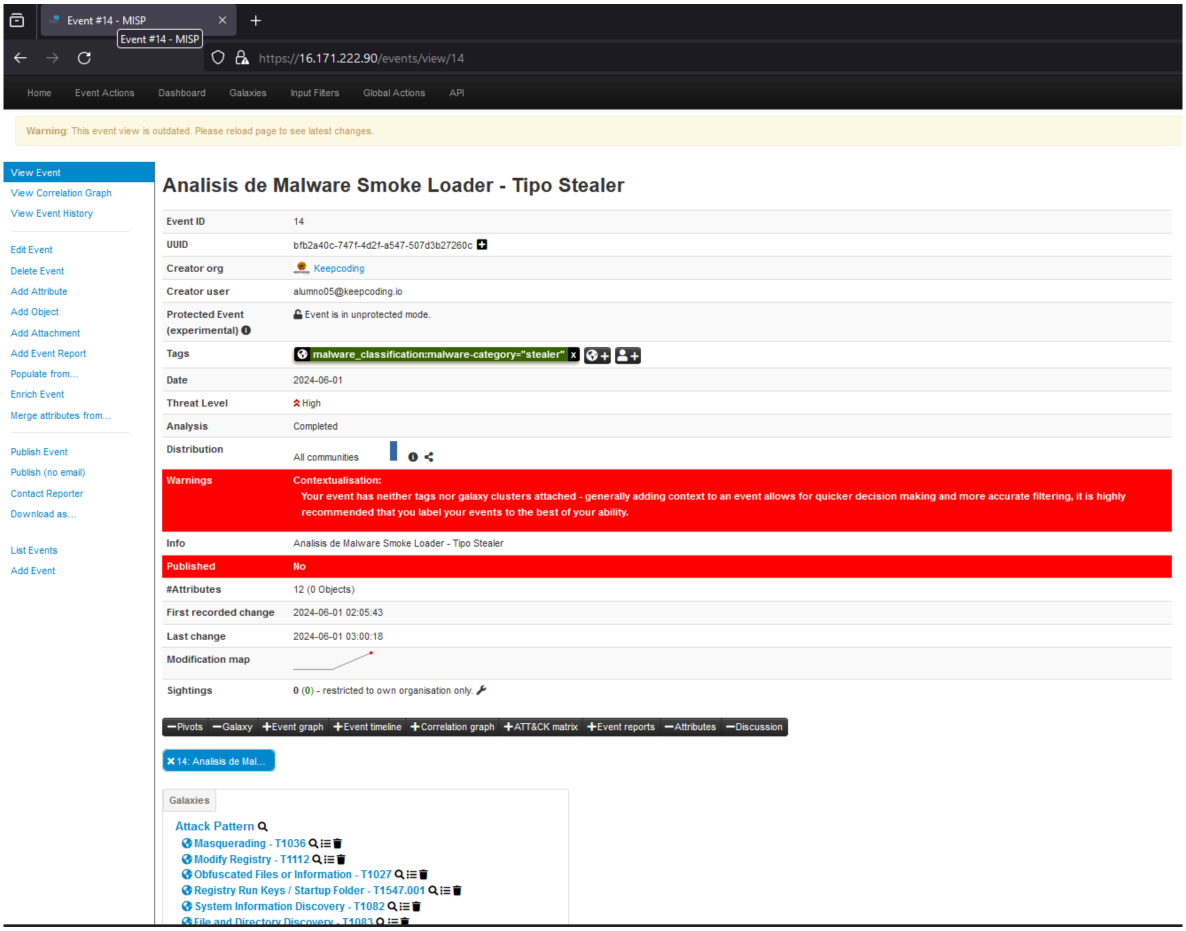
Save	Name :: type	Description	Category	Value	IDS	Disable Correlation
□	**Attachment** attachment	A non-malicious file.	External analysis	Examinar... Ningún archivo seleccionado.	□	□
□	**Malware-sample** malware-sample	The file itself (binary)	Payload delivery	Examinar... Ningún archivo seleccionado.	☑	□
□	**Text** text	Free text value to attach to the file	Other		□	☑
□	**Sha512** sha512	Secure Hash Algorithm 2 (512 bits)	Payload delivery		☑	□
☑	**Sha1** sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	Payload delivery	a723dea176c400de9bdd169b703eb283032ed2cb	☑	□
□	**Pattern-in-file** pattern-in-file	Pattern that can be found in the file	Payload installation		☑	□
☑	**Md5** md5	[Insecure] MD5 hash (128 bits)	Payload delivery	e0e783bba2f8e3f0d2da2bded27eceed	☑	□
☑	**Sha256** sha256	Secure Hash Algorithm 2 (256 bits)	Payload delivery	aaaacef934239	☑	□
□	**Entropy** float	Entropy of the whole file	Other		□	☑
☑	**Filename** filename	Filename on disk	Payload delivery	Original name: Lameros.exe Internal name: Bastard.exe	☑	☑



Sightings 0 (0) - restricted to own organisation only.

Attack Pattern
- Masquerading - T1036
- Modify Registry - T1112
- Obfuscated Files or Information - T1027
- Registry Run Keys / Startup Folder - T1547.001
- System Information Discovery - T1082
- File and Directory Discovery - T1083
- Process Discovery - T1057
- System Owner/User Discovery - T1033
- Security Software Discovery - T1518.001
- Process Injection - T1055
- Query Registry - T1012
- Indicator Removal on Host - T1070
- OS Credential Dumping - T1003
- Data from Local System - T1005
- Application Window Discovery - T1010
- Application Layer Protocol - T1071
- Proxy - T1090
- Native API - T1106
- Email Collection - T1114
- Trusted Developer Utilities Proxy Execution - T1127
- Shared Modules - T1129
- Indirect Command Execution - T1202
- Assign KITs/KIQs into categories - T1228
- Data Destruction - T1485
- Data Encrypted for Impact - T1486
- Virtualization/Sandbox Evasion - T1497
- Steal Web Session Cookie - T1539
- Unsecured Credentials - T1552
- Credentials from Password Stores - T1555
- Archive Collected Data - T1560
- Impair Defenses - T1562
- Hide Artifacts - T1564
- Encrypted Channel - T1573

Malpedia
- SmokeLoader



Warning: This event view is outdated. Please reload page to see latest changes.

Analisis de Malware Smoke Loader - Tipo Stealer

Event ID	14
UUID	bfb2a40c-747f-4d2f-a547-507d3b27260c
Creator org	Keepcoding
Creator user	alumno05@keepcoding.io
Protected Event (experimental)	Event is in unprotected mode.
Tags	malware_classification:malware-category="stealer" x
Date	2024-06-01
Threat Level	High
Analysis	Completed
Distribution	All communities
Warnings	Contextualisation: Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.
Info	Analisis de Malware Smoke Loader - Tipo Stealer
Published	No
#Attributes	12 (0 Objects)
First recorded change	2024-06-01 02:05:43
Last change	2024-06-01 03:00:18
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Attack Pattern

- Masquerading - T1036
- Modify Registry - T1112
- Obfuscated Files or Information - T1027
- Registry Run Keys / Startup Folder - T1547.001
- System Information Discovery - T1082
- File and Directory Discovery - T1083