

An isometric illustration of a digital workspace. In the center, a large white rectangular screen stands on a white platform. Two stylized human figures are on the platform: one in a pink shirt pointing at a target icon on the screen, and another in a green shirt pointing at a floating icon. To the left, a person in a pink shirt sits at a desk with a laptop. To the right, another person in a pink shirt sits on a white block, also using a laptop. The background is a teal gradient with a network of white lines and circular icons containing symbols like a lightbulb, a shopping cart, a padlock, a gear, and a person. The overall theme is digital connectivity and user interaction.

Fray Ávila Hernández

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

Date	Distribution
<input type="text" value="2023-12-10"/>	<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="Smoker loader analizado"/>	
Extends Event	
<input type="text" value="Event UUID or ID. Leave blank if not applicable."/>	
<input type="button" value="Submit"/>	

1.2 Añadimos los objetos

<input checked="" type="checkbox"/>	Sha1 sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	<input type="text" value="Payload delivery"/>	<input type="text" value="6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Pattern-in-file pattern-in-file	Pattern that can be found in the file	<input type="text" value="Payload installation"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<div></div>						
<input checked="" type="checkbox"/>	Md5 md5	[Insecure] MD5 hash (128 bits)	<input type="text" value="Payload delivery"/>	<input type="text" value="fc5e9ebe857d45fa5f578593342ede53"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Sha256 sha256	Secure Hash Algorithm 2 (256 bits)	<input type="text" value="Payload delivery"/>	<input type="text" value="82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Entropy float	Entropy of the whole file	<input type="text" value="Other"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Filename filename	Filename on disk	<input type="text" value="Payload delivery"/>	<input type="text" value="explorer.exe"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	date	orig	category	type	value	page	comment
	2023-12-10		Object name: file				Ma
			References: 0				
<input type="checkbox"/>	2023-12-10		Payload delivery	sha1: sha1	6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c		
<input type="checkbox"/>	2023-12-10		Payload delivery	md5: md5	fc5e9ebe857d45fa5f578593342ede53		
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256: sha256	82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19		
<input type="checkbox"/>	2023-12-10		Payload delivery	filename: filename	explorer.exe		

Objeto creado.

1.3 Añadimos Atributos

Add Attribute

Category

Payload installation

Type

sha256

Distribution

Inherit event

Value

0d297c0f7cde6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f32

Contextual Comment

explorer.exe

☐ For Intrusion Detection System

☐ Batch Import

☐ Disable Correlation

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

Submit

<input type="checkbox"/>	Date	Org	Category	Type	Value	Tags	Guides	Comment	Correlate	Related Events	Feed URL	IO	Disposition
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	12cbb662f357a3be5dac4e19a58c7079cfc6c180ff52db827640f1a3b74c75d			B7C1.exe	<input checked="" type="checkbox"/>	17 18		<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	f3951f0fe95de7deaddae4c07656dfb39ebc46fca7bb07bdf711a886f33d8b86			WerFault.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	015e3f63a4b336ac9dbfa5304eaf2954277a5d2501d52f5b8b67767c96e8df2c			288D.exe	<input checked="" type="checkbox"/>	17 18		<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	93b169fd78f865f3ecd315d176947d8bc5c45794d0334c365818f058e4645c9a			AppLaunch.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	e62f2be0a979e6d7d633ac099e2ce579e3a0b02799c0cbec91cb64e41a020364			regsvr32.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	c7287b7f6d9fe20ab12cc545ad77627e3a37f86a94bca3284693677a7152f6b2			tasklist.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	24f8ba2105b5be091540c801d4ce6471b5d2f28479dc3905cd01236c5f85882b			cmd.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	2df7ac59e0436af254bd931c9bf49ca3a21a43ed4087cadf8ccc7b4ca40aa953			findstr.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	c35f6c7b6388fe6a45a6b5680b133ccc54a3c57b6c0d8a1d9b40359f2c715407			WerFault.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload delivery	sha256	8a02bc37c96f772bf549b576f3d47d399c6d4df018d57dfb94c145a076889b6f			PING.EXE	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2023-12-10		Payload installation	sha256	0d297c0f7cde6c2761880d9d2e9e35a93720aa3460b0e1034111377a70703f32d			explorer.exe	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit

Atributos añadidos.

1.4 Añadimos IPS

Network activity	ip-src	179.25.46.206	   			Inherit
Network activity	ip-src	34.143.166.163	   		16 17	 Inherit
Network activity	ip-src	91.215.85.1	   			Inherit
Network activity	ip-src	181.168.176.36	   			Inherit
Network activity	ip-src	172.67.137.48	   			Inherit

Ips añadidas.

1.5 Añadimos Procesos

Payload delivery	text	Se están utilizando estas herramientas para listar procesos y buscar ciertos procesos en la lista, como "avastui.exe", "avgui.exe", "nswscsvc.exe", "so phoshealth.exe", "wrsa.exe", entre otros.			tasklist.exe y findstr.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit
Payload delivery	text	Un proceso de alojamiento de tareas de Windows.			taskhost.exe (PID 1896)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit
Payload delivery	text	Un proceso relacionado con la instrumentación de administración de Windows.			WmiPrvSE.exe (PID 5188)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit
Payload delivery	text	Varias instancias de "svchost.exe" están ejecutándose. Este es un proceso legítimo de Windows que aloja servicios del sistema.			svchost.exe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit
Payload delivery	text	Un proceso legítimo de Windows que gestiona las credenciales de inicio de sesión.			lsass.exe (PID 1884)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit

1.6 Añadimos Persistencia

Date	Org	Category	Type	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 archivo DLL ubicado en la carpeta temporal del usuario "%TEMP%\942B.dll". Esto podría ser una técnica utilizada por malware para persistencia o ejecución de código malicioso.			regsvr32.exe (PID 4008 y PID 2804					Inherit

1.7 Añadimos Attack pattern

19: Smoker loader ...

Galaxies

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

Boot or Logon Autostart Execution - T1547

Software Packing - T1027.002

Process Discovery - T1057

System Owner/User Discovery - T1033

Disable or Modify Tools - T1562.001

Software Discovery - T1518

Credentials In Files - T1552.001

Process Injection - T1055

Query Registry - T1012

Indicator Removal on Host - T1070

OS Credential Dumping - T1003

Data from Local System - T1005

Application Window Discovery - T1010

PowerShell - T1059.001

Application Layer Protocol - T1071

Proxy - T1090

Multi-hop Proxy - T1090.003

Native API - T1106

Email Collection - T1114

Trusted Developer Utilities Proxy Execution - T1127

Shared Modules - T1129

Indirect Command Execution - T1202

System Binary Proxy Execution - T1218

InstallUtil - T1218.004

Data Destruction - T1485

Data Encrypted for Impact - T1486

Virtualization/Sandbox Evasion - T1497

Smoker loader analizado

Event ID	19
UUID	9a2d5c95-0413-4f5b-8108-7558145b8ad8
Creator org	Keepcoding
Creator user	alumno11@keepcoding.io
Protected Event (experimental)	Event is in unprotected mode.
Tags	malware_classification:malware-category="Trojan" x ms-caro-malware-full:malware-type="TrojanDropper" x
Date	2023-12-10
Threat Level	High
Analysis	Completed
Distribution	This community only
Info	Smoker loader analizado
Published	No
#Attributes	26 (1 Object)
First recorded change	2023-12-10 16:11:17
Last change	2023-12-10 17:32:40
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Evento id:19

<https://13.48.162.234/events/view/19>