

III Bootcamp Full Stack Cibersecurity

Módulo 7 - Malware Analysis



Caso práctico Ticketing

FAME | VIPER | MISP

Marcos Alonso González

alonsogonzalezmarcos@gmail.com

<https://github.com/magalorn>

7 de mayo de 2022

Índice

1. VIPER	3
2. FAME	4
3. MISP	6

1. VIPER

Se han subido dos muestras al gestor de malware **VIPER**:

alumno07

Project marcos

<http://3.133.116.136:8000/project/marcos/>

- Dharma.exe
- 1.bin

La segunda muestra se ha subido ya que en los últimos meses se ha asociado este malware a Dharma. Podríamos estar ante una muestra modificada del malware de Dharma, por lo que sería interesante analizar más en profundidad 1.bin más adelante, si bien en este informe nos centramos en el análisis de Dharma.exe.

The screenshot shows the VIPER web interface. At the top, there's a navigation bar with 'Projects', 'Yara Rules', and 'CLI'. A search bar is present with the text 'Search in all Projects'. The user is logged in as 'alumno07'. Below the navigation bar, the breadcrumb 'Home / marcos' is visible. The main section is titled 'Samples in Project: marcos'. It features an upload area with a 'Choose file' button and an 'Upload' button. Below this, there's a table of samples. The table has columns for '#', 'SHA256', 'Name', 'Mime Type', 'Size', and 'Tags'. Two samples are listed: 'Dharma.exe' (11.5 MB) and '1.bin' (12.5 MB). The 'Dharma.exe' sample has tags 'dharma' and 'ransomware'. The interface also includes pagination controls at the bottom right, showing '1' of 2 entries.

#	SHA256	Name	Mime Type	Size	Tags
1	6fb383dd8ba36381948127d44bd8541e4a1ab8af67b46526ace08458f2498850	Dharma.exe	application/x-dosexec; charset=binary	11.5 MB	dharma ransomware
2	7570a7a6830ade05dcf862d5862f12f12445dbd3c0ad7433d99872849e11c267	1.bin	application/x-dosexec; charset=binary	12.5 MB	





2. FAME

Se ha lanzado sobre **FAME** análisis tanto del fichero Dharma.exe como de la botnet <http://epoolsoft.com> con todos los módulos disponibles.

El funcionamiento de la plataforma es sencillo, para el análisis, en el apartado “Submit” se ofrecen las siguientes opciones:

- Subir una muestra del fichero a analizar
- Analizar una url
- Analizar un hash

En este caso, se ha subido el fichero Dharma.exe y se ha analizado <http://epoolsoft.com>, la URL de la botnet hallada en el análisis con el resto de herramientas.

Analyses Most recent first						
	DATE	STATUS	OBJECT	TARGET	PROBABLE NAMES	EXTRACTIONS
	2022-05-08 12:52	finished	6d3d62a4cff19b4f2cc7ce9027c33be8 E906FA3D51E86A61741B3499145A114E98FB7C56			
	2022-05-07 16:32	finished	cb7eeca95af26dcd1112c4bd4e4d27e epoolsoft.com			
	2022-05-07 16:32	finished	85482ee33979a7d9f3eb935135b2aac3 http://epoolsoft.com			
	2022-05-07 16:25	finished	928e37519022745490d1af1ce6f336f7 Dharma.exe			

Sin embargo no se ha encontrado información de interés diferente a la extraída con el resto de herramientas utilizadas en el análisis. Puede verse la información obtenida en estos enlaces:

alumno07@keepcoding.io

Dharma.exe: <http://13.58.26.224/analyses/62769d93b4ee101273de0f8f/>

<http://epoolsoft.com>: <http://13.58.26.224/analyses/62769f1db4ee101273de0f96/>

A destacar, es que FAME no detecta la URL de la botnet como maliciosa.

FAME incluye integración con Virus Total, muestra como en el caso de Dharma.exe, la herramienta detecta en la mayoría de marcas de AVs la muestra como malware.

Execution Path

Tags & modules

virustotal_public exiftool

exiftool flare_capa virustotal_public urlscan polyswarm document_preview email_headers eml extract msg office_macros url_download peepdf url_preview xlm_deobfuscator legacyzip RTF reversing

Status: ✔ finished ● Executed ● Ongoing ● Pending ● Waiting ● Cancelled

Virus Total Report

Detailed Results

SCORE

55 / 69

SCAN DATE

2022-04-19 14:53:38

PERMALINK

<https://www.virustotal.com/gui/file/6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850/detection/f-6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850-1650380018>

DETECTIONS

Engine	Detection	Version
Lionic	Trojan.Win32.AntiVM.trEF	20220419
Elastic	malicious (high confidence)	20220302
DrWeb	BAT.AddUser.77	20220419
MicroWorld-eScan	Adware.GenericKD.34375248	20220419
FireEye	Generic.mg.928e375190227454	20220419

3. MISP

Plataforma utilizada por la comunidad de analistas de malware para compartir la información de las muestras analizadas.

Cuenta con un sistema de cumplimentación de campos y diferentes apartados donde se puede incluir información para crear eventos.

Alumno07

Event ID 12

<https://18.119.159.89/events/view/12>

The screenshot displays the MISP web interface for viewing a specific event. On the left, a sidebar menu offers various actions like 'View Event', 'Edit Event', and 'Add Attribute'. The main content area shows the event details for 'Ransomware Dharma' (Event ID 12). Key information includes the UUID, creator (Keepcoding), date (2022-05-07), threat level (High), and analysis (Initial). The event is currently unpublished, highlighted by a red bar. Below the main details, there are sections for attributes, change history, and sightings. At the bottom, a navigation bar allows switching between different views like Pivots, Galaxy, Event graph, etc.

Ransomware Dharma	
Event ID	12
UUID	330f6867-eeaa-44fe-a59d-9970f2a7b932
Creator org	Keepcoding
Creator user	alumno07@keepcoding.com
Protected Event (experimental)	Event is in unprotected mode.
Tags	🌐, 👤
Date	2022-05-07
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Ransomware Dharma
Published	No
#Attributes	34 (0 Objects)
First recorded change	2022-05-08 10:45:42
Last change	2022-05-08 18:54:27
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Navigation: — Pivots — Galaxy + Event graph + Event timeline + Correlation graph + ATT&CK matrix + Event reports — Attributes — Discussion

Event ID: 12: Ransomware D...

En este caso, con la muestra Dharma.exe, se ha incluido en el evento, entre otra, la siguiente información:

- Atributos: Se ha añadido información de las categorías External Analysis, Payload delivery, Artifacts Dropped, Network Activity, Persistence mechanism.

Para incluir información de atributos, basta con pulsar “Add Attribute” en el menu lateral izquierdo y posteriormente elegir categoria, tipo e incluir la información.

<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
<input type="checkbox"/>	2022-05-08		External analysis	url	https://www.virustotal.com/gui/file/6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850/detection				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		External analysis	url	https://www.virustotal.com/graph/6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		External analysis	url	https://www.hybrid-analysis.com/sample/6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850?environmentId=100				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Payload delivery	attachment	Dharma.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Artifacts dropped	process-state	%WINDIR%\System32\net.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Artifacts dropped	process-state	%WINDIR%\System32\ssadmin.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Artifacts dropped	process-state	C:\ac\EVER\SearchHost.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Artifacts dropped	process-state	C:\ac\mssq2.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Artifacts dropped	process-state	C:\ac\nc123.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Payload delivery	sha512	8040195ab2b2e15c9d5fa13a47a61c709738d1cf5e2108e48fedf3408e5bad5f2c5f523f170f6a80cb33a4f5612d3d60dd343d028e55dc08cd26ed2347c				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Payload delivery	malware-type	Ransomware PE32 executable (GUI) Intel 80386, for Microsoft Windows				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Payload delivery	filename	dharma.exe				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Payload delivery	sha256	6fb303dd8ba36381948127d44bd8541e4a1ab8af07b46526ace08458f2498850				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Payload delivery	sha1	b7840242393013f2c4c136ac7407e332be075702				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Payload delivery	md5	928e37519022745490d1af1ce6f336f7				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Network activity	user-agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.DC; .NET4.0F; InfoPath.3)				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Network activity	ip-src	38.63.60.243				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	bftchvhpwike.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	ybtodsueovrdim.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	aunnepymeymlgu.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	jkehgayzbdw1.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	bthcjegvyanfeucqk.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	pxslubysyhrrodzj.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	yqopjbrwxsigv.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	gnbrnwywmkzrl.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	plloataboupgjfts.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	nnuyulterjgh.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	mssq2.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	xtqycabccagmthzqd.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Persistence mechanism	filename	vzanprvpdmqse.sys				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Artifacts dropped	mutex	{Sessions}\1\BaseNamedObjects\Local\ZonesCacheCounterMutex {Sessions}\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex Local\ZonesCacheCounterMutex Local\ZonesLockedCacheCounterMutex				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		
<input type="checkbox"/>	2022-05-08		Network activity	domain	www.epoolsoft.com				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		*
<input type="checkbox"/>	2022-05-08		Payload delivery	yara	YARA signature "dharma_ransomware" classified file "1sass.exe" as "dharma.crysis ransomware" based on indicators: "C:\crisis\Release\IPDB\payload.pdb" (Author: Marc Rivero Hybrid Analysis)				<input checked="" type="checkbox"/>			<input type="checkbox"/>	Inherit	(0/0)		

- Galaxies: En la Attack Pattern Galaxy, se incluyen las tácticas de la Matriz MITRE ATT&CK que se han encontrado en el análisis del malware. Se han encontrado en este caso 24 coincidencias.

Galaxies

Attack Pattern Q

- Modify Registry - T1112 Q
- System Information Discovery - T1082 Q
- Remote Desktop Protocol - T1021.001 Q
- Software Packing - T1027.002 Q
- Winlogon Helper DLL - T1547.004 Q
- Process Injection - T1055 Q
- Peripheral Device Discovery - T1120 Q
- Query Registry - T1012 Q
- Screen Capture - T1113 Q
- Application Window Discovery - T1010 Q
- Windows Management Instrumentation - T1047 Q
- Process Hollowing - T1055.012 Q
- Credential API Hooking - T1056.004 Q
- Command and Scripting Interpreter - T1059 Q
- Windows Command Shell - T1059.003 Q
- Domain Groups - T1069.002 Q
- File Deletion - T1070.004 Q
- Web Protocols - T1071.001 Q
- Local Account - T1087.001 Q
- Inhibit System Recovery - T1490 Q
- Disable or Modify System Firewall - T1562.004 Q
- Hidden Files and Directories - T1564.001 Q
- NTFS File Attributes - T1564.004 Q
- Service Execution - T1569.002 Q

« previous next » view all

Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool

mitre-pre-attack	mitre-attack	mitre-mobile-attack	Initial access (19 items)	Execution (38 items)	Persistence (10 items)	Privilege escalation	Defense evasion (167 items)	Credential access (55 items)	Discovery (42 items)	Lateral movement (23 items)	Collection (36 items)	Command and control	Exfiltration (17 items)
Cloud Accounts	Command and Scripting Interpreter	Winlogon Helper DLL	Process Hollowing	Disable or Modify System Firewall	Credential API Hooking	Application Window Discovery	Remote Desktop Protocol	Credential API Hooking	Web Protocols	Automated Exfiltration			
Compromise Hardware Supply Chain	Service Execution	Accessibility Features	Process Injection	File Deletion	/etc/passwd and /etc/shadow	Domain Groups	Application Access Token	Screen Capture	Application Layer Protocol	Data Transfer Size Limits			
Compromise Software Dependencies and Development Tools	Windows Command Shell	Account Manipulation	Winlogon Helper DLL	Hidden Files and Directories	ARP Cache Poisoning	Local Account	Component Object Model and Distributed COM	ARP Cache Poisoning	Asymmetric Cryptography	Exfiltration Over Alternative Protocol			
Compromise Software Supply Chain	Windows Management Instrumentation	Active Setup	Abuse Elevation Control Mechanism	Modify Registry	AS-REP Roasting	Peripheral Device Discovery	Distributed Component Object Model	Adversary-in-the-Middle	Bidirectional Communication	Exfiltration Over Asymmetric Encrypted Non-Confidential Protocol			
Default Accounts	AppleScript	Add Office 365 Global Administrator Role	Access Token Manipulation	NTFS File Attributes	Adversary-in-the-Middle	Query Registry	Exploitation of Remote Services	Archive Collected Data	Commonly Used Port	Exfiltration Over Bluetooth			
Domain Accounts	At (Linux)	Add-Ins	Accessibility Features	Process Hollowing	Bash History	System Information Discovery	Internal Spearphishing	Archive via Custom Method	Communication Through Removable Media	Exfiltration Over C Channel			
Drive-by Compromise	At (Windows)	Additional Cloud Credentials	Active Setup	Process Injection	Brute Force	Account Discovery	Lateral Tool Transfer	Archive via Library	DNS	Exfiltration Over Other Network Medium			
Exploit Public-Facing Application	Component Object Model	AppCert DLLs	AppCert DLLs	Software Packing	Cached Domain Credentials	Browser Bookmark Discovery	Pass the Hash	Archive via Utility	DNS Calculation	Exfiltration Over Physical Medium			
External Remote Services	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Abuse Elevation Control Mechanism	Cloud Instance Metadata API	Cloud Account	Pass the Ticket	Audio Capture	Data Encoding	Exfiltration Over Symmetric Encrypted Non-Confidential Protocol			

Se han incluido en este ticketing una pequeña parte de la información que puede subirse a la plataforma sobre la muestra analizada, ya que MISP cuenta con un gran abanico de posibilidades para incluir información de diferentes maneras, incluso con la subida del fichero que contiene la muestra sobre la que se ha compartido la información.

Una vez finalizado el evento, puede publicarse para compartirlo con la comunidad de usuarios de MISP.