

ANÁLISIS DE MALWARE

INCIDENTES DE CIBERSEGURIDAD



ERIC SERRANO MARÍN
UNIDAD 4

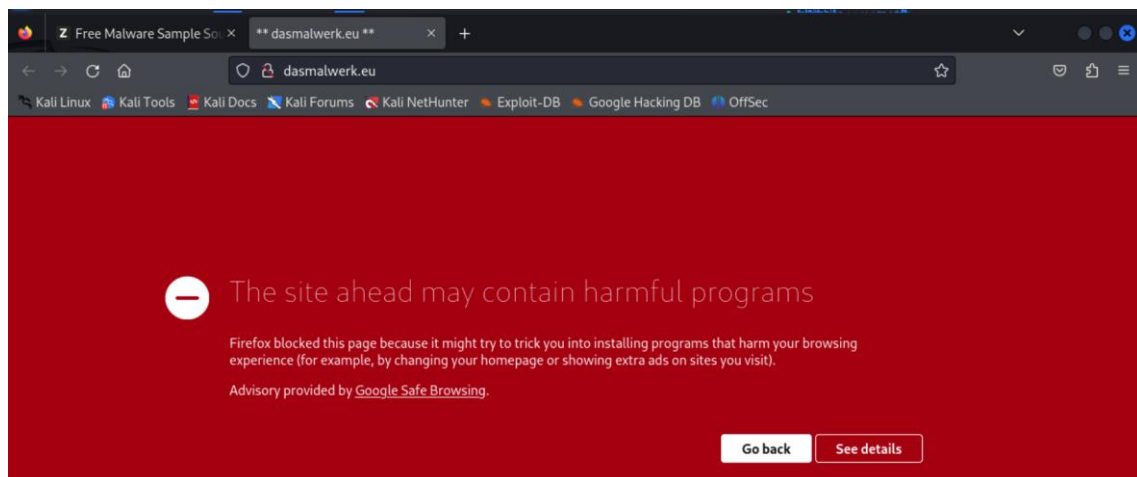
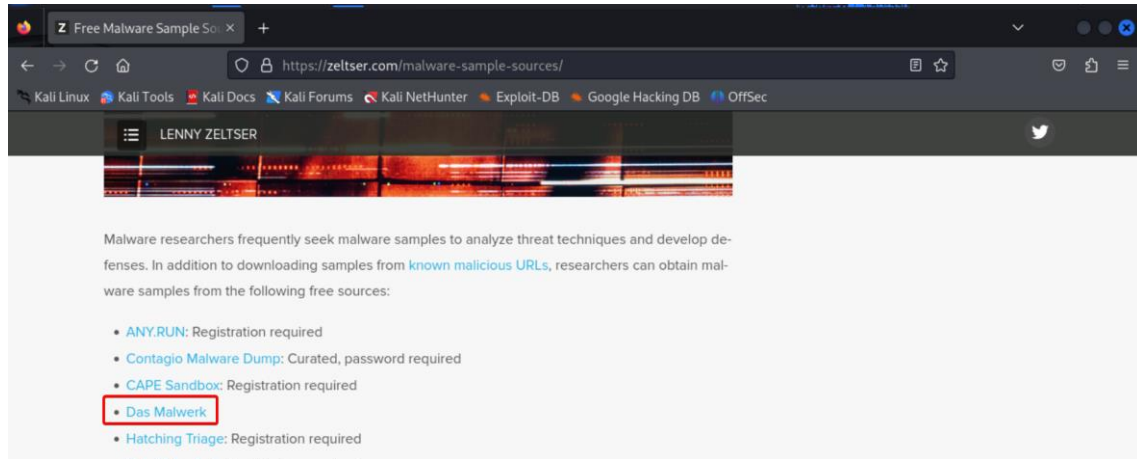
Contenido

1. Descargando malware.....	2
2. Analizando con virustotal, urlscan.io, hybrid análisis y herramienta online cuckoo sandbox.	3
Virusotal URL.....	3
Virusotal File	4
Urlscan.io.....	4
Hybrid analysis URL	5
Cuckoo sandbox url	10
Cuckoo sandbox file	10

1. Descargando malware.

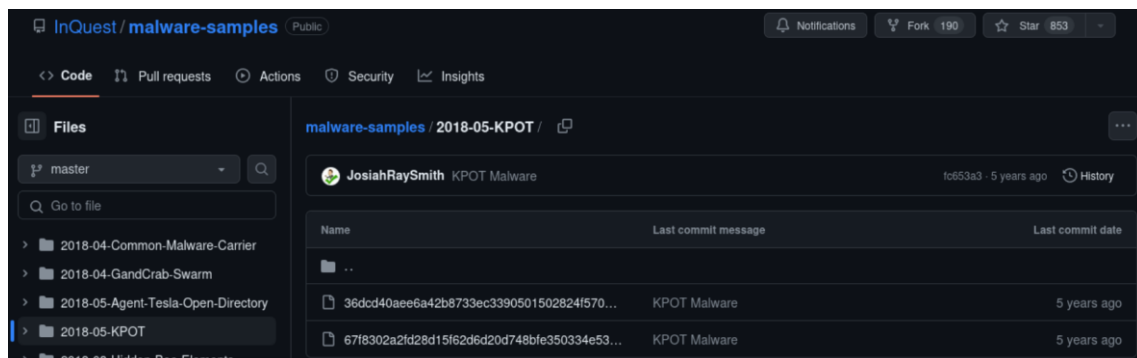
<https://zeltser.com/malware-sample-sources/>

Primero vamos a probar usando una página web.



Para la prueba de archivos vamos a descargar los siguientes:

<https://github.com/InQuest/malware-samples/tree/master/2018-05-KPOT>



2. Analizando con virustotal, urlscan.io, hybrid análisis y herramienta online cuckoo sandbox.

Virustotal URL

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE **URL** SEARCH

<http://dasmalwerk.eu/>

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

5 / 91

5 security vendors flagged this URL as malicious

Reanalyze Search Graph API

http://dasmalwerk.eu/
dasmalwerk.eu

Status: 200 Content type: text/html, charset=utf-8 Last Analysis Date: 2 months ago

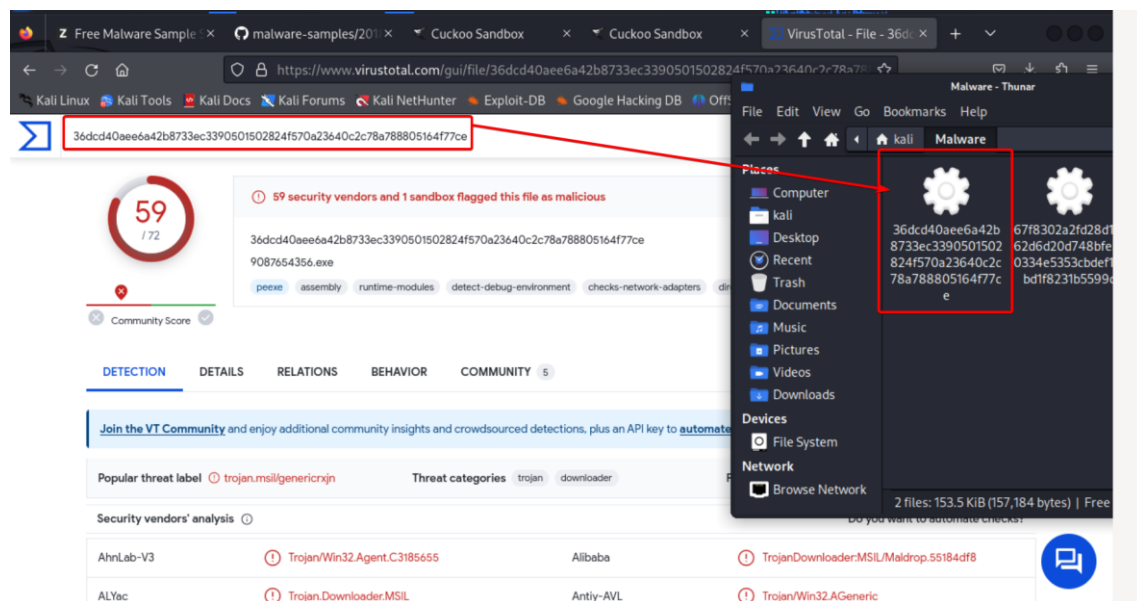
Community Score

DETECTION DETAILS CONTENT COMMUNITY 1

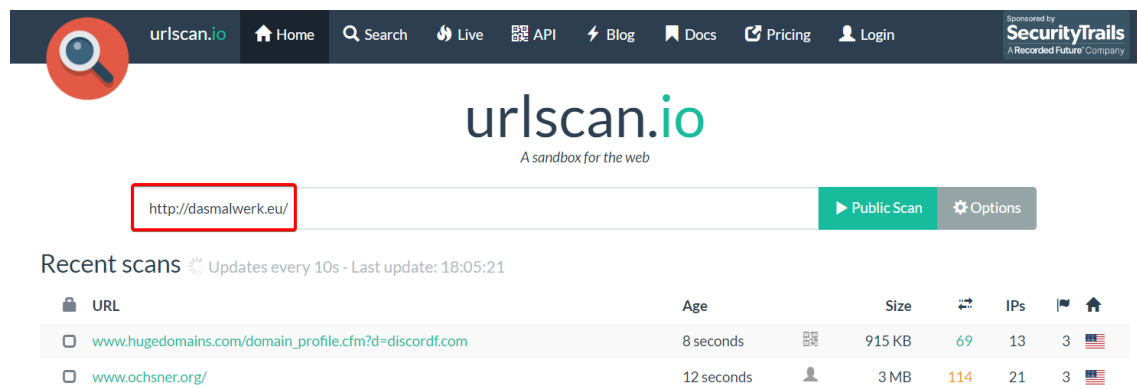
[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis Do you want to automate checks?

CyRadar	Malicious	Fortinet	Malware
Google Safebrowsing	Malicious	Lumu	Malware
Seclookup	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
ALLabs (MONITORAPP)	Clean	AlienVault	Clean

Virustotal File

Gif del resultado: <https://i.imgur.com/NiAJ8ls.gif>

Urlscan.io

Ninguno de los enlaces me ha funcionado escaneando con urlscan, y los que me han funcionado salen sin vulnerabilidades

Aquí dejo un ejemplo.

www.team-cymru.com

34.149.87.45 Public Scan

URL: <https://www.team-cymru.com/bogon-networks>

Submission: On March 06 via manual (March 6th 2024, 3:14:34 pm UTC) from ES — Scanned from ES

Summary HTTP 115 Redirects Links Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted 17 IPs in 3 countries across 14 domains to perform 115 HTTP transactions. The main IP is 34.149.87.45, located in Kansas City, United States and belongs to GOOGLE-CLOUD-PLATFORM, US. The main domain is www.team-cymru.com. TLS certificate: Issued by Sectigo RSA Domain Validation Secure ... on February 28th 2024. Valid for: 3 months.

[www.team-cymru.com](#) scanned 177 times on urlscan.io Show Scans 177

urlscan.io Verdict: No classification ✓

Live information

Screenshot Live screenshot Full image

The Bogan Reference

Hybrid analysis URL



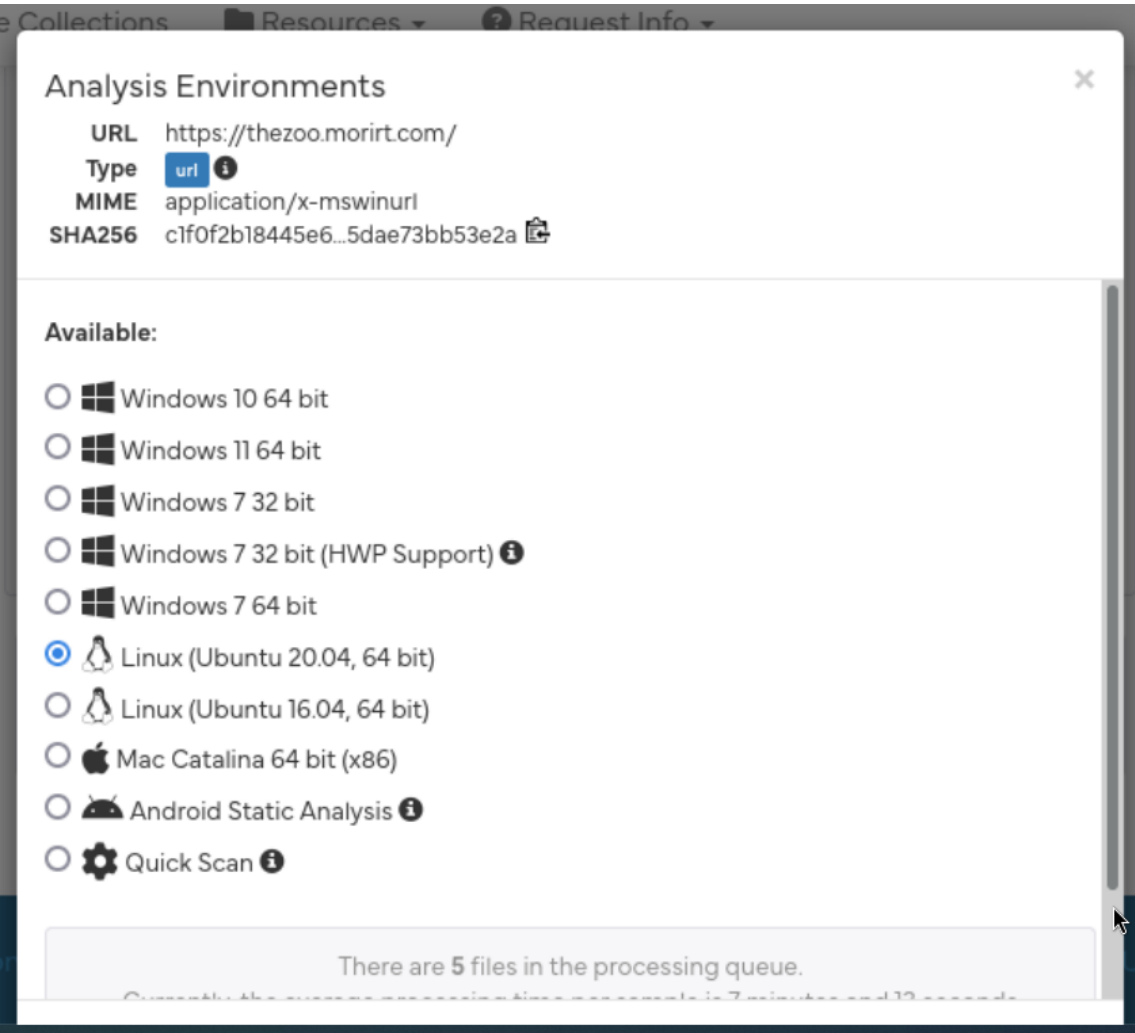
File/URL File Collection Report Search YARA Search String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Drag & Drop For Instant Analysis

or

Analyze



100.0%

malicious

2 of 2 are detected as malicious

GET STARTED WITH A FREE TRIAL

100.0%

malicious

2 of 2 are detected as malicious

Files

Show 10 entries

Search:

File name	SHA256	Tags	AV Result	Sandbox Report	Verdict
67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d	67f8302a..31b5599d	evasive	96% Malware	✓	malicious
36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce	36dcd40a..164f77ce	-	92% Trojan.Generic	✓	malicious

Showing 1 to 2 of 2 entries

Previous

1

Next

HYBRID ANALYSIS

SandboxQuick ScansFile CollectionsResourcesRequest Info

Request Report Deletion

Analysis Overview

Submission name:hxtps://thezoo.morirt.com/

Size:50B

Type:uri

Mime:application/x-mswinurl

Operating System:Windows

Last Anti-Virus Scan:03/05/2024 19:06:59 (UTC)

Last Sandbox Report:03/05/2024 19:06:25 (UTC)

malicious

Threat Score: 100/100

LinkTwitterE-Mail

Anti-Virus Results

Up-to-date

urlscan.io

CLEAN

Uri Scan Analysis

Last Update: 03/05/2024 19:06:59 (UTC)

View Details

ScamAdviser

3%

Domain Scam Score

Last Update: 03/05/2024 19:06:59 (UTC)

View Details

CleanDNS

0

Alleged Domain Abuse Reports

Last Update: 03/05/2024 19:06:59 (UTC)

View Details: N/A

HYBRID ANALYSIS

SandboxQuick ScansFile CollectionsResourcesRequest Info

Request Report Deletion

Part-RU

daa85471dbc8c994eed3725f3076aaf6c4e298b963fb712e53eb0fa2dc1e789

malicious

bnpl_driver.js

1f4f1041a49d486b94e3596a637b77e91f5c294648a413761f2662f34a005f0

no specific threat

bnpl.html

c8224f4a6c4924f88e89d7c878ba1fcfaba657894d408eff8cb255f004317d0e

no specific threat

load-hub-ii8n.bundle.js

no specific threat

Falcon Sandbox Reports

MALICIOUS

https://thezoo.morirt.com/

Analyzed on: 01/14/2024 07:41:36 (UTC)

Environment: Windows 10 64 bit

Threat Score: 100/100

AV Detection: Marked as clean

Indicators: 10

Network:

NO SPECIFIC THREAT

https://thezoo.morirt.com/

Analyzed on: 06/28/2020 22:17:20 (UTC)

Environment: Windows 7 32 bit

Threat Score: N/A

AV Detection: Marked as clean

Indicators: 4

Network:

REJECTED

https://thezoo.morirt.com/

Analyzed on: 03/05/2024 19:06:25 (UTC)

Environment: Linux (Ubuntu 20.04, 64 bit)

If you believe this is incorrect behavior, please contact support@hybrid-analysis.com providing the SHA256 and sample

Página 7 | 11

Hybrid analysis file

The image shows the Hybrid Analysis website interface. At the top, the logo consists of a red and blue circular arrow icon followed by the text "HYBRID ANALYSIS". Below the logo, there is a navigation bar with links: "File/URL", "File Collection" (highlighted with a red box and a red circle with the number 1), "Report Search", "YARA Search", and "String Search".



The main content area features a large text block: "Here you can upload and share your file collections. Receive instant threat analysis using **CrowdStrike Falcon Static Analysis (ML)**, reputation lookups, AV engines, static analysis and more. All files uploaded will be made available to the community YARA/String search." Below this text is a large dashed rectangular box with two interlocking gears in the center and the text "Drag & Drop For Instant Analysis" at the bottom. A red box and a red circle with the number 2 highlight this area.

Below the main content area, there is a screenshot of the website's interface for a specific file collection. The URL in the browser is "https://www.hybrid-analysis.com/file-collection/65e/6c9aas34afc/42094c/2". The page title is "Unknown Files Collection". It shows a "Copy SHA256" button and a "malicious" status. The "Analysis Overview" section includes "Anti-Virus Scanner Results" and "Files". The "Anti-Virus Results" section shows two circular progress indicators for "CrowdStrike Falcon" and "MetaDefender", both at 100.0% and labeled as "malicious".

On the right side of the page, there is a "Latest News" section with several articles, including "HijackLoader Expands Techniques to Improve Defense Evasion", "IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations", "New Container Exploit: Rooting Non-Root Containers with CVE-2023-2640 and CVE-2023-32629, aka GameOver(tty)", and "The Windows Restart Manager: How It Works and How It Can Be Hijacked, Part 2".

CollectionsResourcesRequest Info

Getting Things Ready

File	Mime	State
 36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce (74.5 KiB)	application/x-dosexec	✓
 67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d (79.0KiB)	application/x-dosexec	✓


Collection Name (optional)

Your file collection name

Your Comment (optional)

This is an example comment with a #tag ...

100% (2/2)

Submit

Cuckoo sandbox url

✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
4520739	05/03/2024 20:48	http://dasmalwerk.eu/	ie	1 ✓ reported
Done				

Summary

URL Details

URL

http://dasmalwerk.eu/

Score

This url is **very suspicious**, with a score of 8.3 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Category	Started	Completed	Duration	Routing	Logs
URL	March 5, 2024, 8:48 p.m.	March 5, 2024, 8:51 p.m.	159 seconds	Internet	Show Analyzer Log Show Cuckoo Log

Signatures

- Allocates read-write-execute memory (usually to unpack itself) (50 out of 299 events)
- Changes read-write memory protection to read-execute (probably to avoid detection when setting all RWX flags at the same time) (1 event)
- Uses Windows utilities for basic Windows functionality (1 event)
- Resumed a suspended thread in a remote process potentially indicative of process injection (2 events)
- File has been identified by 5 AntiVirus engines on VirusTotal as malicious (5 events)

Screenshots

Cuckoo sandbox file

Configure your Analysis

Full Memory Dump: ☒ If enabled, has been enabled, process an entire VM memory dump with it.

Enforce Timeout: ☐

Enable Simulated Human Interaction: ☐

Reset **Analyze**

File	Size
36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a78880516477ce	74.5 KiB
67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d	79.0 KiB

Selection: 2/2

✔ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
4520768	📅 05/03/2024 ⌚ 21:13	36dcd40aee6a42b8733ec3390501502824f570a23640c2c78a788805164f77ce	exe	● completed
4520769	📅 05/03/2024 ⌚ 21:13	67f8302a2fd28d15f62d6d20d748bfe350334e5353cbdef112bd1f8231b5599d	exe	● completed
Done				