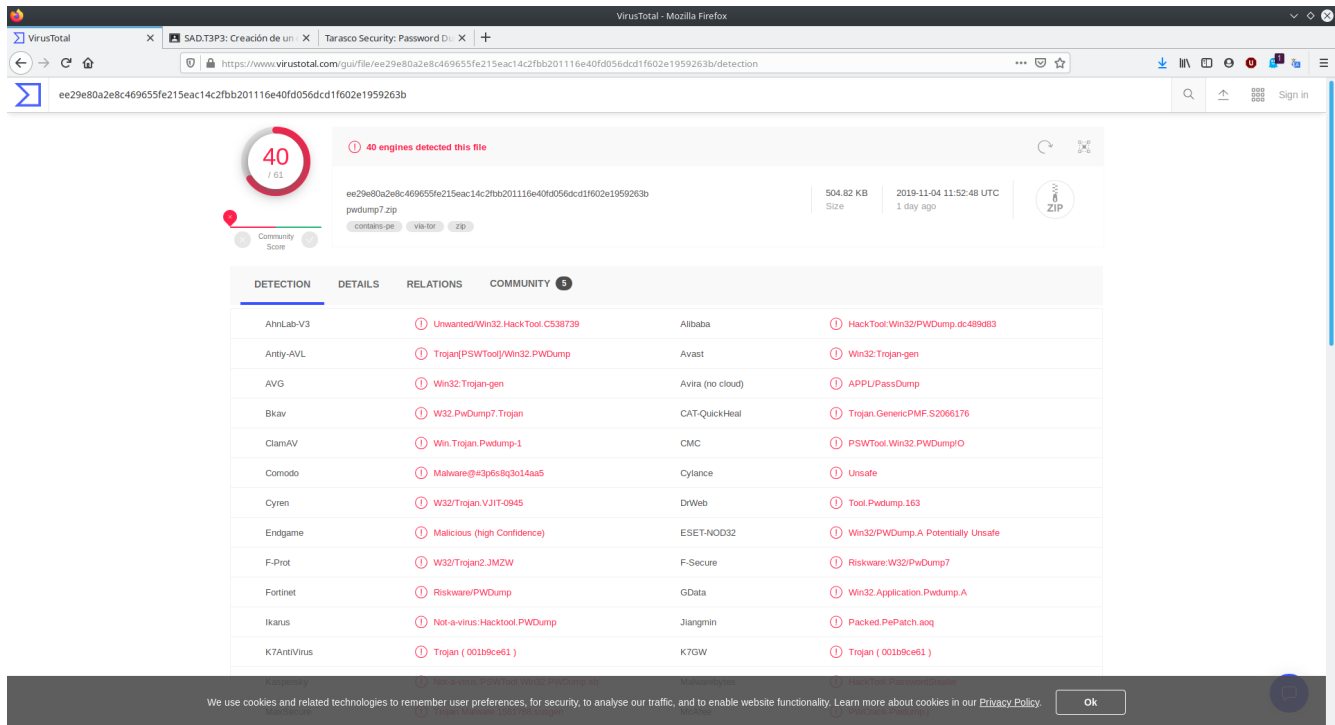


Práctica 1: Análisis de malware y url maliciosas

En esta practica como no compromete ningún riesgo para el sistema lo realizamos sin ninguna maquina virtual.

Nos dirigimos a <https://www.virustotal.com/gui/home/upload> y subimos Pwdump7.zip para analizarlo y estos son los resultados y las diferentes amenazas que detecta.



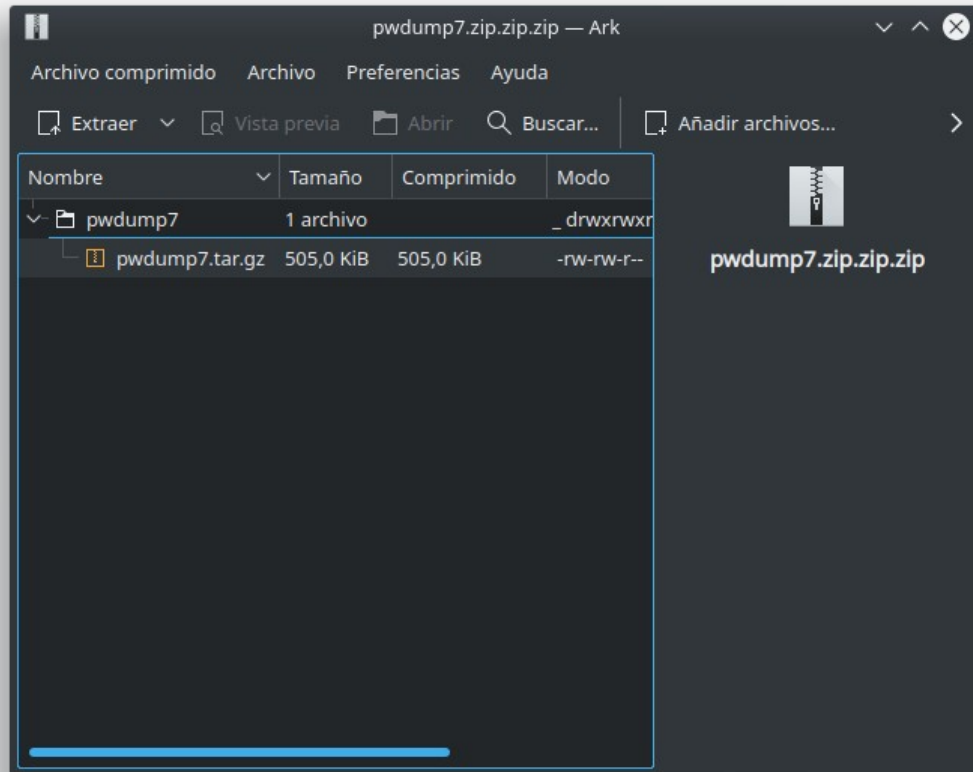
The screenshot shows the VirusTotal web interface in a Mozilla Firefox browser. The URL bar displays the file's hash and the detection page. The file 'pwdump7.zip' (504.82 KB) was uploaded on 2019-11-04. A circular progress indicator shows 40 engines detected the file. Below this, a table lists the detections from various security engines.

DETECTION	DETAILS	RELATIONS	COMMUNITY
AhnLab-V3	Unwanted:Win32.HackTool.C538739	Alibaba	HackTool:Win32/PWDump.dc489d83
Antiy-AVL	Trojan(PSWTool)/Win32.PWDump	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	APPL/PassDump
Bkav	W32.PwDump7.Trojan	CAT-QuickHeal	Trojan.Generic.PMF.S2066176
ClamAV	Win.Trojan.Pwdump-1	CMC	PSWTool.Win32.PWDump.O
Comodo	Malware@#3p6s8q3o14aa5	Cylance	Unsafe
Cyren	W32/Trojan.VJIT-0945	DrWeb	Tool.Pwdump.163
Endgame	Malicious (high Confidence)	ESET-NOD32	Win32/PWDump.A Potentially Unsafe
F-Prot	W32/Trojan2.JM2W	F-Secure	Riskware:W32/PwDump7
Fortinet	Riskware/PWDump	GData	Win32.Application.Pwdump.A
Ikarus	Not-a-virus:Hacktool.PWDump	Jiangmin	Packed.PePatch.aq
K7AntiVirus	Trojan (001b8ce61)	K7GW	Trojan (001b8ce61)

At the bottom of the page, a cookie consent banner is visible, stating: "We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Policy." with an "Ok" button.

Práctica 1: Análisis de malware y url maliciosas

Ahora comprimiremos varias veces Pwdump7.zip para ver si lo detecta en este caso desde el entorno grafico es muy fácil. Lo vamos metiendo en un directorio llamado Pwdump7.zip.zip y lo comprimimos. Así repitiendo 2 o 3 veces. Hasta tener Pwdump7.zip.zip.zip que anteriormente lo comprimí con .tar.gz Vamos el proposito esta hecho



Práctica 1: Análisis de malware y url maliciosas

Lo volvemos a subir a la web de <https://www.virustotal.com>

Screenshot of VirusTotal analysis results for file 6a6bee37361c0a09c6413cf821af84cc9e62efd1f30bbdb5590606debd06ba9.

26 / 58 engines detected this file

6a6bee37361c0a09c6413cf821af84cc9e62efd1f30bbdb5590606debd06ba9
pwdump7.zip.zip.zip

505.25 KB Size | 2019-11-05 14:31:50 UTC a moment ago

Community Score

DETECTION	DETAILS	RELATIONS	COMMUNITY
AhnLab-V3	UnwantedWin32.HackTool.CS38739	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	APPU/PassDump
CAT-QuickHeal	Trojan.Generic.PMF.52066176	ClamAV	Win.Trojan.Pwdump-1
Comodo	Malware@k3p6s8q3o14aa5	Cyren	W32/Trojan.VJIT-0945
DrWeb	Tool.Pwdump.163	ESET-NOD32	Win32/PWDump.A Potentially Unsafe
F-Prot	W32/Trojan2.JM2W	F-Secure	Riskware:W32/PwDump7
Fortinet	Riskware/PWDump	GData	Win32.Application.Pwdump.A
Ikarus	Not-a-virus:Hacktool.PWDump	Jiangmin	Packed PePatch.aog
Kaspersky	Not-a-virus:PSWTool.Win32.PWDump.sb	McAfee	PWCrack-Pwdump.j
McAfee-GW-Edition	PWCrack-Pwdump.j	Microsoft	HackTool.Win32/PWDump.I
NANO-Antivirus	Riskware.Win32.Hashdump.cvgfj	Panda	Hacktool/PWDump
TrendMicro	HKTL_PWDUMP	VBA32	Backdoor-Hupigon

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Policy](#). Ok

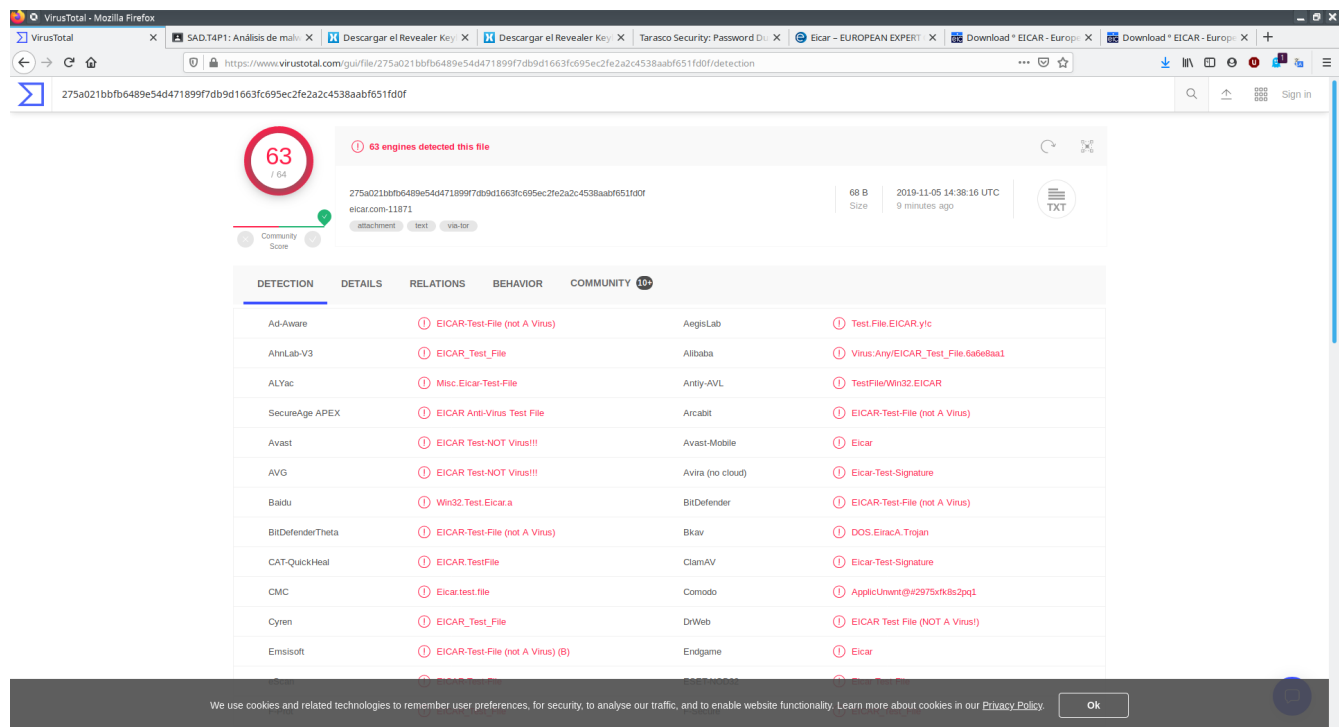
Esta vez a detectado menos amenazas pese a ello es efectivo por detectarla.

Práctica 1: Análisis de malware y url maliciosas

Ahora vamos a usar el archivo de eicar.com que recordemos que es un malware de muestra para ver lo que detecta lo sacamos de aquí

<http://2016.eicar.org/download/eicar.com>

Y estos son los resultados.



63 engines detected this file

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
eicar.com-11871

68 B Size
2019-11-05 14:38:16 UTC
9 minutes ago

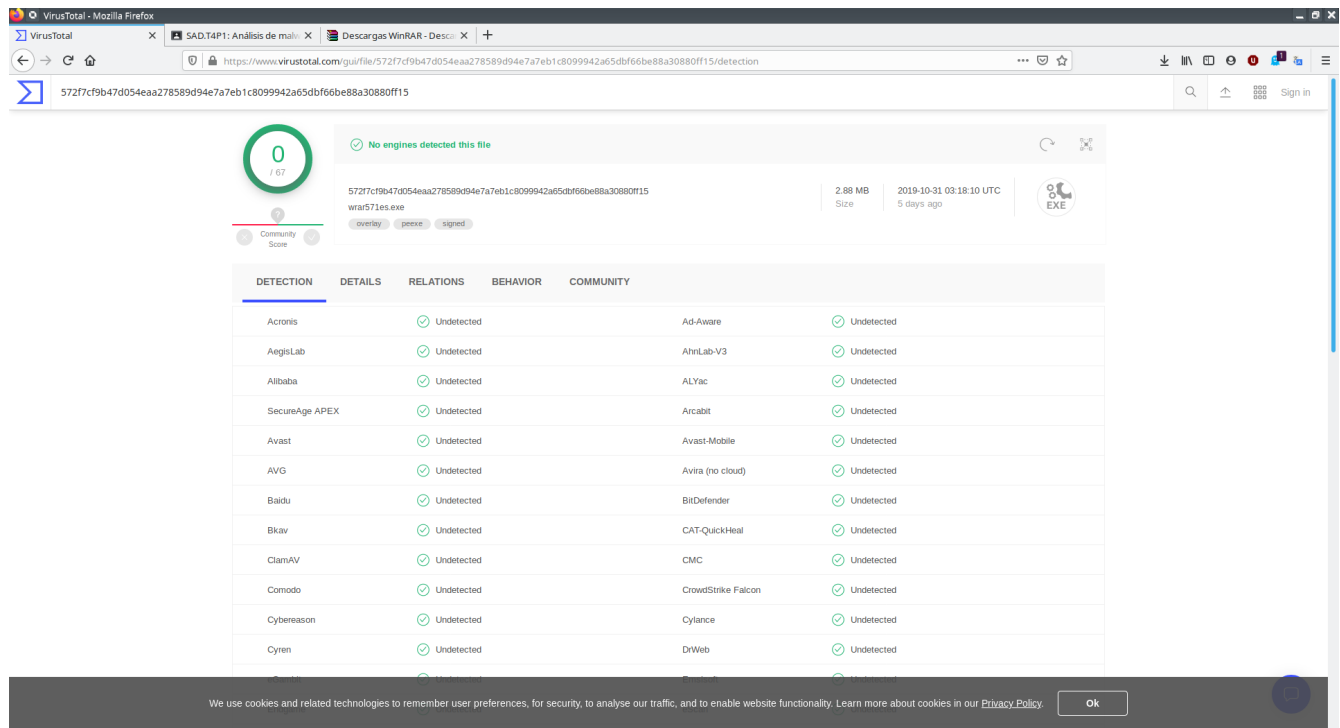
Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware		ⓘ EICAR-Test-File (not A Virus)		AegisLab ⓘ Test-File.EICAR.ytc
AhnLab-V3		ⓘ EICAR_Test_File		Alibaba ⓘ Virus:Any/EICAR_Test_File.6a6ebaa1
ALYac		ⓘ Misc.Eicar-Test-File		Antiy-AVL ⓘ TestFile/Win32.EICAR
SecureAge APEX		ⓘ EICAR Anti-Virus Test File		Arcabit ⓘ EICAR-Test-File (not A Virus)
Avast		ⓘ EICAR Test-NOT Virus!!!		Avast-Mobile ⓘ Eicar
AVG		ⓘ EICAR Test-NOT Virus!!!		Avira (no cloud) ⓘ Eicar-Test-Signature
Baidu		ⓘ Win32.Test.Eicar.a		BitDefender ⓘ EICAR-Test-File (not A Virus)
BitDefenderTheta		ⓘ EICAR-Test-File (not A Virus)		Bkav ⓘ DOS.EIrac.Trojan
CAT-QuickHeal		ⓘ EICAR.Test-File		ClamAV ⓘ Eicar-Test-Signature
CMC		ⓘ Eicar.test.file		Comodo ⓘ ApplicUnwnt@w2975xfk8s2pg1
Cyren		ⓘ EICAR_Test_File		DnWeb ⓘ EICAR Test File (NOT A Virus!)
Emsisoft		ⓘ EICAR-Test-File (not A Virus) (8)		Endgame ⓘ Eicar

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Policy. Ok

Práctica 1: Análisis de malware y url maliciosas

Ahora pasaremos un instalador de Winrar mismo que es un .exe



The screenshot shows the VirusTotal web interface in a Mozilla Firefox browser. The URL bar displays the file's hash and detection status. The main content area shows a green circle with a '0' indicating no detections. Below this, a table lists various antivirus engines and their results, all showing 'Undetected'.

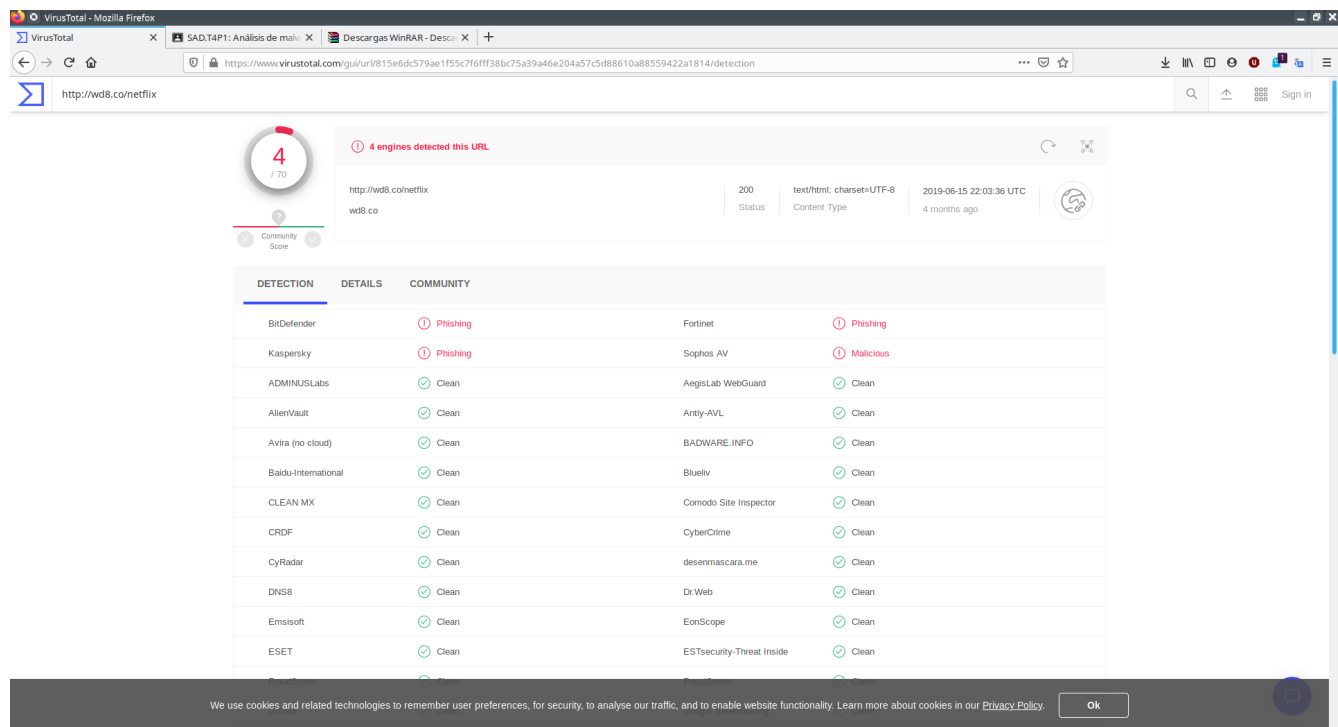
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis	Undetected	Ad-Aware	Undetected	
AegisLab	Undetected	AhnLab-V3	Undetected	
Alibaba	Undetected	ALYac	Undetected	
SecureAge APEX	Undetected	Arcabit	Undetected	
Avast	Undetected	Avast-Mobile	Undetected	
AVG	Undetected	Avira (no cloud)	Undetected	
Baidu	Undetected	BitDefender	Undetected	
Bkav	Undetected	CAT-QuickHeal	Undetected	
ClamAV	Undetected	CMC	Undetected	
Comodo	Undetected	CrowdStrike Falcon	Undetected	
Cybereason	Undetected	Cylance	Undetected	
Cyren	Undetected	DrWeb	Undetected	

Comparándolo con los archivos anteriores este no contiene ninguna amenaza de ningún tipo por lo tanto es seguro. Y mas que esta descargado de sus sitio oficial.

Práctica 1: Análisis de malware y url maliciosas

Ahora vamos analizar sitios web no es nada raro estar navegando y colarse por un sitio que pueda comprometer nuestra seguridad. Sobre todo si queremos descargar pelis, musica .mp3 etc. Recordemos que es algo ilegal pero siempre hay sitios que ofrecerán esto pero recordemos que nada es gratis. Y los riesgos que podemos tener es este. Desde que usen nuestra CPU para minar monedas hasta intentar sonsacarnos contraseñas, numeros de tarjeta, datos personales, etc.

Primero analizamos la web de la practica <http://wd8.co/netflix>



The screenshot shows the VirusTotal web interface in a Mozilla Firefox browser. The address bar displays the URL <https://www.virustotal.com/gui/url/815e6dc579ae1f55c7f6ff38bc75a39a46e204a57c5d88610a88559422a1814/detection>. The page title is "http://wd8.co/netflix". A large red circle with the number "4" indicates that 4 engines detected this URL. Below this, a table shows the detection results from various antivirus engines. The table has three columns: "DETECTION", "DETAILS", and "COMMUNITY". The "DETECTION" column lists the antivirus engines, and the "DETAILS" column shows the detection results (e.g., "Phishing", "Clean", "Malicious"). The "COMMUNITY" column shows the community score (e.g., "Clean", "Phishing", "Malicious").

DETECTION	DETAILS	COMMUNITY
BitDefender	Phishing	Phishing
Kaspersky	Phishing	Malicious
ADMINUSLabs	Clean	Clean
Avira (no cloud)	Clean	Clean
Baidu-International	Clean	Clean
CLEAN MX	Clean	Clean
CRDF	Clean	Clean
CyRadar	Clean	Clean
DNSB	Clean	Clean
Emissoft	Clean	Clean
ESET	Clean	Clean
Fortinet	Phishing	Phishing
Sophos AV	Malicious	Malicious
AegisLab WebGuard	Clean	Clean
Antiy-AVL	Clean	Clean
BADWARE.INFO	Clean	Clean
Blueliv	Clean	Clean
Comodo Site Inspector	Clean	Clean
CyberCrime	Clean	Clean
desenmascara.me	Clean	Clean
Dr.Web	Clean	Clean
EonScope	Clean	Clean
ESTSecurity-Threat Inside	Clean	Clean

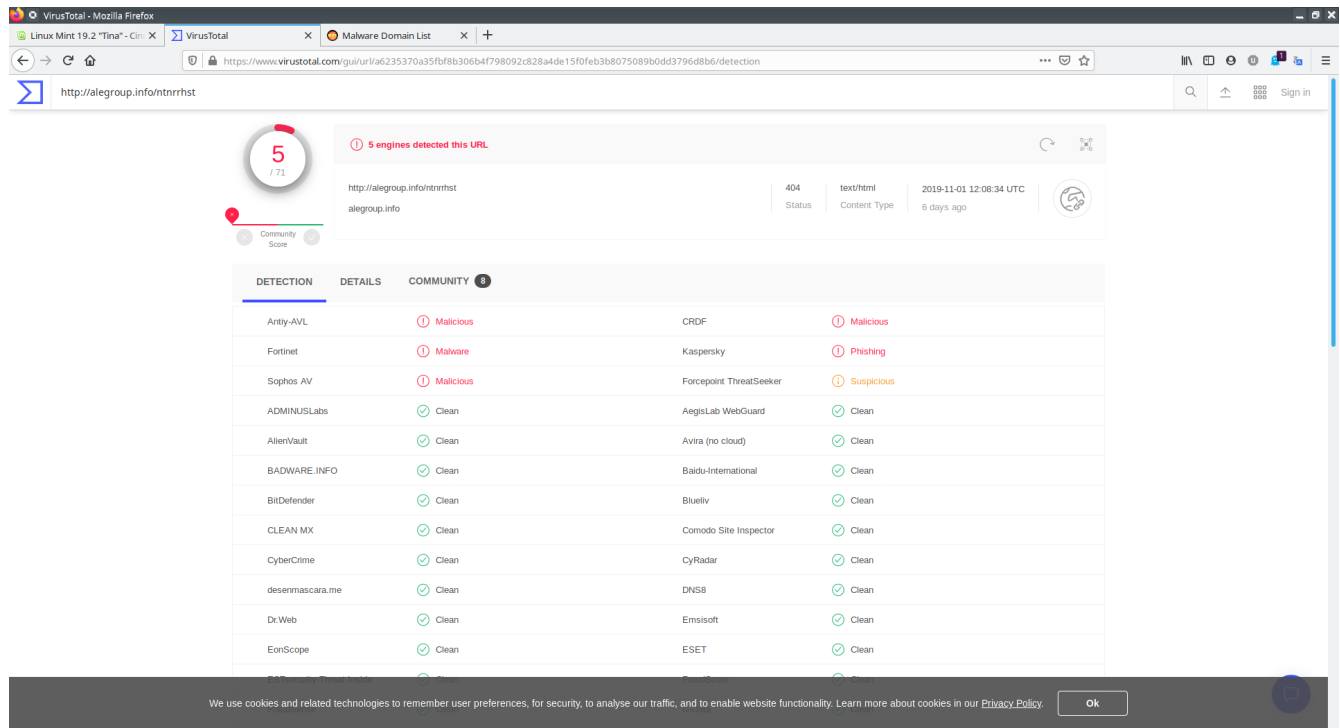
La verdad es que aunque parece mentira que intente ser muy irresponsable y colarme por sitios de descargas gratis , peliculas y series, etc. Y no encontré nada supongo que es como la ley de Murphy cuando lo buscas no lo encuentras y un día sin querer lo encuentras o mejor dicho te puedes infectar en algún virus.

De todas forma he buscado un poco y encontré una web interesante donde contiene una lista de URL con malware.

<https://www.malwaredomainlist.com/mdl.php>

Práctica 1: Análisis de malware y url maliciosas

Cualquiera de los enlaces descritos en esta web son peligrosos así que hay que ir con ojo.



The screenshot shows the VirusTotal web interface for the URL `http://alegroup.info/ntrrhst`. The URL is marked as detected by 5 engines. The page includes a summary section with the URL, status (404), content type (text/html), and a timestamp (2019-11-01 12:08:34 UTC). Below this is a table with three tabs: DETECTION, DETAILS, and COMMUNITY. The DETECTION tab is active, showing a list of security engines and their results.

DETECTION	DETAILS	COMMUNITY	
Antiy-AVL	Malicious	CRDF	Malicious
Fortinet	Malware	Kaspersky	Phishing
Sophos AV	Malicious	Forcepoint ThreatSeeker	Suspicious
ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AlienVault	Clean	Avira (no cloud)	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
BitDefender	Clean	Blueliv	Clean
CLEAN MX	Clean	Comodo Site Inspector	Clean
CyberCrime	Clean	CyRadial	Clean
desenmascara.me	Clean	DNIS	Clean
Dr.Web	Clean	Emsisoft	Clean
EonScope	Clean	ESET	Clean