


java.z.jar


malicious

This report is generated from a file or URL submitted to this webservice on December not enough data to reliably determine 14th 2015 10:51:04 (UTC)

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

Report generated by [Falcon Sandbox](#) © Hybrid Analysis


-  Overview
-  Sample unavailable
-  Downloads ▼
-  External Reports ▼
-  Re-analyze
-  Hash Not Seen Before
-  Report False-Positive



**Attention:** this analysis ran with the legacy *Usermode Monitor*. It is highly recommended to use the Kernelmode Monitor.

 Request Report Deletion

## Incident Response

 Risk Assessment

<b>Remote Access</b>	Uses network protocols on unusual ports
<b>Persistence</b>	Modifies auto-execute functionality by setting/creating a value in the registry
<b>Fingerprint</b>	Reads system information using Windows Management Instrumentation Commandline (WIMC)
<b>Network Behavior</b>	Contacts 1 domain and 1 host. <a href="#">View all details</a>

## Indicators

 Not all malicious and suspicious indicators are displayed. [Get your own cloud service or the full version to view all details.](#)

Malicious Indicators 4

**External Systems**

Sample was identified as malicious by a large number of Antivirus engines

Sample was identified as malicious by at least one Antivirus engine

**Network Related**

Uses network protocols on unusual ports

**Spyware/Information Retrieval**

Accesses potentially sensitive information from local browsers

Suspicious Indicators 3

### Incident Response

#### Indicators

- Malicious (4)
- Suspicious (3)
- Informative (4)

File Details

Screenshots (1)

Hybrid Analysis (3)

Network Analysis

Extracted Strings

Extracted Files (0)

Notifications

Community (0)

[Back to top](#)









### 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

<div><div>HYBRID ANALYSIS</div><div><div>▼</div><div>▼</div><div></div><div>▼</div><div> Request Info ▼</div></div></div> <div><div></div><div></div><div>▼</div></div>	<div><div>Spyware/Information Retrieval</div><div>Reads system information using Windows Management Instrumentation Commandline (WIMC)▼</div><div>Informative4</div><div>General</div><div>Contacts domains▼</div><div>Contacts server▼</div><div>Creates mutants▼</div><div>Spawns new processes▼</div></div>
--	--

## File Details

All Details: ☐ Off

 java.z.jar

Filename

Size

Type

Description

Architecture

SHA256

java.z.jar

248KiB (253942 bytes)

java

compressed

jar

Zip archive data, at least v2.0 to extract

WINDOWS


4be06ecd234e2110bd615649fe4a6fa95403979acf889d7e45a78985eb50acf9

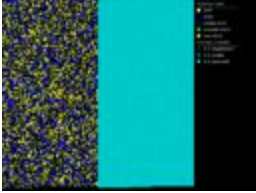
Resources

Icon

Visualization

Input File (PortEx)





Classification (TrID)

78.3% (.JAR) Java Archive

21.6% (.ZIP) ZIP compressed archive

## Screenshots




## Hybrid Analysis

 **Tip:** Click an analysed process below to view more


### 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](#)





HYBRID


ANALYSIS

 ▾


 ▾

 ▾

 ▾



 Request Info

▾



×

▾


 **wmic.exe** wmic /node:localhost /namespace:\\root\SecurityCenter2 path FirewallProduct get /format:list (PID: 3116) 

 Logged Script Calls	 Logged Stdout	 Extracted Streams	 Memory Dumps
 Reduced Monitoring	 Network Activity	 Network Error	 Multiscan Match

## Network Analysis


### DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
alps2015.ddns.net	179.178.243.99	-	 Brazil

### Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
179.178.243.99	1340 TCP	-	 Brazil


### Contacted Countries



### HTTP Traffic

No relevant HTTP requests were made.

## Extracted Strings



Search

All Details: 

Off

All Strings (4)

Interesting (3)

javaw.exe (1)

screen\_0.png (1)

wmic.exe (2)

-jar "%SAMPLEDIR%\java.z.jar"

wmic /node:localhost /namespace:\\root\SecurityCenter2 path AntiVirusProduct get /format:list

wmic /node:localhost /namespace:\\root\SecurityCenter2 path FirewallProduct get /format:list

### 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](#)

## Notifications

Runtime

▼

## Community

ⓘ There are no community comments.

ⓘ You must be logged in to submit a comment.



### 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](#)