HYBRID ANALYSIS

java.z.jar

malicious

not enough data to reliably determine

This report is generated from a file or URL submitted to this webservice on December 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

Post | Link | E-Mail

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Looking for file context ...
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

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

Indicators

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

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

Installation/Persistance

Modifies auto-execute functionality by setting/creating a value in the registry

Remote Access Related

Contains references to WMI/WMIC

Spyware/Information Retrieval

Reads system information using Windows Management Instrumentation Commandline (WIMC)

Informative

4

General

Contacts domains

Contacts server

Spawns new processes

File Details

All Details: Off

java.z.jar

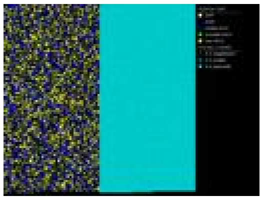
Filename	java.z.jar
Size	248KiB (253942 bytes)
Type	java compressed jar
Description	Zip archive data, at least v2.0 to extract
Architecture	WINDOWS
SHA256	4be06ecd234e2110bd615649fe4a6fa95403979acf889d7e45a78985eb50acf9

Resources

Icon

Visualization

Input File (PortEx)



Classification (TrID)

- 78.3% (.JAR) Java Archive
- 21.6% (.ZIP) ZIP compressed archive

Screenshots

ℹ Loading content, please wait...

HYBRID
ANALYSIS

Hybrid Analysis

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

Analysed 3 processes in total (System Resource Monitor).

- javaw.exe -jar "%SAMPLEDIR%\java.z.jar" (PID: 2300)
  - wmic.exe wmic /node:localhost /namespace:\\root\SecurityCenter2 path AntiVirusProduct get /format:list (PID: 2828)
  - 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 Activityy	⚠ 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

HYBRID ANALYSIS

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
```

Extracted Files

No significant files were extracted.

Notifications

Community

❗ There are no community comments.

❗ You must be logged in to submit a comment.