

IMG.94751700 PDF_original.jar 

This report is generated from a file or URL submitted to this webservice on November 6th 2017 08:18:58 (UTC)

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

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

malicious

Threat Score: 75/100

AV Detection: 45%

Labeled as: Trojan.Maljava

#java_adwind

#jrat

#evasive

Post

Link

E-Mail

-  Overview

 Sample unavailable

 Downloads ▼

 External Reports ▼

 Re-analyze


 Hash Not Seen Before

 No similar samples

 Report False-Positive

 Request Report Deletion

Incident Response

 Risk Assessment

Persistence

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

Spawns a lot of processes

Writes data to a remote process


Fingerprint

Reads system information using Windows Management Instrumentation Commandline (WMIC)

Reads the active computer name

Reads the cryptographic machine GUID

Indicators

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

Malicious Indicators 5	
External Systems	
Detected Emerging Threats Alert	▼
Sample was identified as malicious by at least one Antivirus engine	▼
General	
The analysis extracted a file that was identified as malicious	▼
Installation/Persistence	
Writes data to a remote process	▼
Unusual Characteristics	
Spawns a lot of processes	▼

Suspicious Indicators 16	
--------------------------	--

Incident Response

Indicators

- Malicious (5)
- Suspicious (16)
- Informative (9)

File Details

Screenshots (1)

Hybrid Analysis (29)

Network Analysis

Extracted Strings

Extracted Files (15)

Notifications

Community (1)

[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

Page 1 of 8

HYBRID ANALYSIS	
Request Info	
Creates guarded memory regions (anti-debugging trick to avoid memory dumping)	
Cryptographic Related	
References key cryptographic functions	
Environment Awareness	
Found a reference to a WMI query string known to be used for VM detection	
Reads the active computer name	
Reads the cryptographic machine GUID	
Installation/Persistence	
Drops executable files	
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 (WMIC)	
Unusual Characteristics	
Installs hooks/patches the running process	
Reads information about supported languages	
Hiding 4 Suspicious Indicators	
All indicators are available only in the private webservice or standalone version	
Informative9	
External Systems	
Sample was identified as clean by Antivirus engines	
General	
Creates a writable file in a temporary directory	
Creates mutants	
Launches a VBS file	
Reads Windows Trust Settings	
Runs shell commands	
Spawns new processes	
Installation/Persistence	


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](#)

File Details

All Details:

Off

IMG.94751700 PDF_original.jar

Filename

IMG.94751700 PDF_original.jar

Size

509KiB (521579 bytes)

Type

java

compressed

jar

Description


Java archive data (JAR)

Architecture

WINDOWS


SHA256

ba86fa0d4b6af2db0656a88b1dd29f36fe362473ae8ad04255c4e52f214a541c



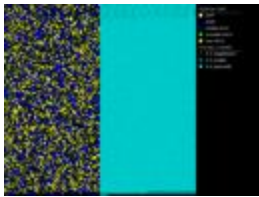
Resources

Icon



Visualization

Input File (PortEx)




Classification (TrID)

100.0% (.ZIP) ZIP compressed archive

Screenshots





Hybrid Analysis



Tip:



Click an analysed process below to view more details.


Analysed 29 processes in total ([System Resource Monitor](#)).


javaw.exe -jar "C:\ba86fa0d4b6af2db0656a88b1dd29f36fe362473ae8ad04255c4e52f214a541c.jar" (PID: 3212) 


java.exe -jar %TEMP%_0.068614639798144752542616253131176441.class (PID: 3860)


Hash Seen Before


cmd.exe /C cscript.exe %TEMP%\Retrive2420117266672210551.vbs (PID: 308) 


cscript.exe %TEMP%\Retrive2420117266672210551.vbs (PID: 4076) 


cmd.exe /C cscript.exe %TEMP%\Retrive3480961498146581831.vbs (PID: 2200) 


cscript.exe %TEMP%\Retrive3480961498146581831.vbs (PID: 300) 


cmd.exe (PID: 2084) 

cmd.exe /C cscript.exe %TEMP%\Retrive2646804049303142888.vbs (PID: 3804) 

cscript.exe %TEMP%\Retrive2646804049303142888.vbs (PID: 312) 

cmd.exe /C cscript.exe %TEMP%\Retrive2670234531104625201.vbs (PID: 3992) 

cscript.exe %TEMP%\Retrive2670234531104625201.vbs (PID: 3996) 

xcopy.exe "xcopy "%PROGRAMFILES%\Java\jre1.8.0_25" "%APPDATA%\Oracle\" /e (PID: 3944) 

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](#)

Page 3 of 8

The screenshot displays the Hybrid Analysis interface. At the top, there is a search bar with a magnifying glass icon and a close button (X). Below the search bar, there is a 'Hash Seen Before' button. The main area shows a process tree for 'java.exe'. The tree structure is as follows:

- java.exe -jar %TEMP%_0.127476670696220488692148369551433214.class (PID: 2704)
 - Hash Seen Before
 - cmd.exe /C cscript.exe %TEMP%\Retrive6218171138404779966.vbs (PID: 2992) [icon]
 - cscript.exe %TEMP%\Retrive6218171138404779966.vbs (PID: 3024) [icon]
 - cmd.exe /C cscript.exe %TEMP%\Retrive4681301751082619848.vbs (PID: 3096) [icon]
 - cscript.exe %TEMP%\Retrive4681301751082619848.vbs (PID: 3208) [icon]
 - cmd.exe (PID: 3100) [icon]
 - cmd.exe /C cscript.exe %TEMP%\Retrive8824404834342482190.vbs (PID: 2720) [icon]
 - cscript.exe %TEMP%\Retrive8824404834342482190.vbs (PID: 2832) [icon]
 - cmd.exe /C cscript.exe %TEMP%\Retrive752908523483486178.vbs (PID: 2772) [icon]
 - cscript.exe %TEMP%\Retrive752908523483486178.vbs (PID: 2732) [icon]
 - cmd.exe (PID: 2864) [icon]
 - WMIC.exe WMIC /Node:localhost /Namespace:\\root\\cimv2 Path Win32_PnpSigned Driver Get /Format:List (PID: 3064) [icon]

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

Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

No relevant hosts were contacted.

HTTP Traffic

No relevant HTTP requests were made.

Suricata Alerts

Event	Category	Description	SID
185145.45149 -> local:55956 (TCP)	A Network Trojan was detected	ET TROJAN Possible Adwind SSL Cert (assylia.sInc)	2020728

 ET rules applied using Suricata. Find out more about proofpoint ET Intelligence [here](#).

Extracted Strings


Search

All Details: ☐ Off







⬇ Download All Memory Strings (2.4KiB)

- | | | | | |
|--------------------|----------------------------|--------------------------|--------------------|--|
| All Strings (439) | Interesting (303) | Windows60053420231541... | attrib.exe (2) | network.pcap (26) |
| reg.exe (1) | xcopy.exe (1) | cscript.exe (8) | javaw.exe:3212 (1) | ba86fa0d4b6af2db0656a... |
| javaw.exe (2) | java.exe (2) | cmd.exe (8) | screen_0.png (3) | Retrive752908523483486... test.txt (1) |
| javaw.exe:2584 (1) | Retrive6218171138404779... | WMIC.exe (1) | ID.txt (2) | |


```
"reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v cRwUMdaPVwP /t REG_EXPAND_SZ /d "\"%APPDATA%\Oracle\bin\javaw.exe\" -jar \"%USERPROFILE%\sgazsBZvxHC\GKPKtwfSplg.ddKgDj\""/f
```





























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](#)

	 ▾	 ▾		 ▾	 Request Info ▾	<div><div>Q</div><div>×</div><div>▾</div></div>
%TEMP%\Retrive4681301751082619848.vbs						
%TEMP%\Retrive6218171138404779966.vbs						
%TEMP%\Retrive752908523483486178.vbs						
%TEMP%\Retrive8824404834342482190.vbs						
(Ljava/lang/String;)V						

Extracted Files

 Displaying 14 extracted file(s). The remaining 1 file(s) are available in the full version and XML/JSON reports.

Malicious		9
 Retrive2420117266672210551.vbs		
<div><div> Overview</div><div> Download Disabled</div><div> VirusTotal Report</div><div> Metadefender Report</div><div> Hash Seen Before</div></div>		
Size	276B (276 bytes)	
Type	<div>text</div>	
Description	ASCII text, with CRLF line terminators	
AV Scan Result	Labeled as "Trojan.Generic" (7/83)	
Runtime Process	java.exe (PID: 3860)	
MD5	3bdfd33017806b85949b6faa7d4b98e4 	
SHA1	f92844fee69ef98db6e68931adfaa9a0a0f8ce66 	
SHA256	9da575dd2d5b7c1e9bab8b51a16cde457b3371c6dcdb0537356cf1497fa868f6 	
 Retrive2646804049303142888.vbs		
<div><div> Overview</div><div> Download Disabled</div><div> VirusTotal Report</div><div> Metadefender Report</div><div> Hash Seen Before</div></div>		
Size	276B (276 bytes)	
Type	<div>text</div>	
Description	ASCII text, with CRLF line terminators	
AV Scan Result	Labeled as "Trojan.Generic" (7/83)	
Runtime Process	cscript.exe (PID: 312)	
MD5	3bdfd33017806b85949b6faa7d4b98e4 	
SHA1	f92844fee69ef98db6e68931adfaa9a0a0f8ce66 	
SHA256	9da575dd2d5b7c1e9bab8b51a16cde457b3371c6dcdb0537356cf1497fa868f6 	
 Retrive2670234531104625201.vbs		
<div><div> Overview</div><div> Download Disabled</div><div> VirusTotal Report</div><div> Metadefender Report</div><div> Hash Seen Before</div></div>		
Size	281B (281 bytes)	
Type	<div>text</div>	
Description	ASCII text, with CRLF line terminators	
AV Scan Result	Labeled as "Trojan.Generic" (4/78)	
Runtime Process	javaw.exe (PID: 3212)	
MD5	a32c109297ed1ca155598cd295c26611 	
SHA1	dc4a1fdbaad15ddd6fe22d3907c6b03727b71510 	
SHA256	45bfe34aa3ef932f75101246eb53d032f5e7cf6d1f5b4e495334955a255f32e7 	
 Retrive3480961498146581831.vbs		

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

Retrive4681301751082619848.vbs

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Hash Seen Before

Size

281B (281 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

AV Scan Result

Labeled as "Trojan.Generic" (4/78)

Runtime Process

java.exe (PID: 2704)

MD5

a32c109297ed1ca155598cd295c26611

SHA1

dc4a1fdbaad15ddd6fe22d3907c6b03727b71510

SHA256

45bfe34aa3ef932f75101246eb53d032f5e7cf6dlf5b4e495334955a255f32e7

Retrive6218171138404779966.vbs

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Hash Seen Before

Size

276B (276 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

AV Scan Result

Labeled as "Trojan.Generic" (7/83)

Runtime Process

java.exe (PID: 2704)

MD5

3bdfd33017806b85949b6faa7d4b98e4

SHA1

f92844fee69ef98db6e6893ladfaa9a0a0f8ce66

SHA256

9da575dd2d5b7c1e9bab8b51a16cde457b3371c6dcdb0537356cf1497fa868f6

Retrive752908523483486178.vbs

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Hash Seen Before

Size

281B (281 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

AV Scan Result

Labeled as "Trojan.Generic" (4/78)

Runtime Process

cscript.exe (PID: 2732)

MD5

a32c109297ed1ca155598cd295c26611

SHA1

dc4a1fdbaad15ddd6fe22d3907c6b03727b71510

SHA256

45bfe34aa3ef932f75101246eb53d032f5e7cf6dlf5b4e495334955a255f32e7

Retrive8824404834342482190.vbs

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Hash Seen Before

Size

276B (276 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

AV Scan Result

Labeled as "Trojan.Generic" (7/83)

Runtime Process

cscript.exe (PID: 2832)

MD5

3bdfd33017806b85949b6faa7d4b98e4

SHA1

f92844fee69ef98db6e6893ladfaa9a0a0f8ce66

SHA256

9da575dd2d5b7c1e9bab8b51a16cde457b3371c6dcdb0537356cf1497fa868f6

Windows6005342023154142644.dll

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Hash Seen Before

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](#)

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](#)