


IMG.94751700 PDF_original.jar 

malicious

This report is generated from a file or URL submitted to this webservice on November 6th 2017 08:18:58 (UTC) Threat Score: 75/100
AV Detection: 45%

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Labeled as: Trojan.Maljava

Report generated by Falcon Sandbox © Hybrid Analysis

#java_adwind #jrat #evasive

Overview

Sample unavailable

Downloads

External Reports

Re-analyze

Looking for file context ...

Looking for similar samples ...

Report False-Positive


Request Report Deletion

Post

Link

E-Mail

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



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
Anti-Detection/Stealthyness	
Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)	▼
Anti-Reverse Engineering	
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	




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 subservice or standalone version	
Informative 9	
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	▼



Installation/Persistence	
Dropped files	▼
Touches files in the Windows directory	▼

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 

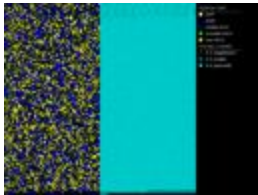
Resources

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](#)).





WMIC.exe WMIC /Node:localhost /Namespace:\\root\\cimv2 Path Win32_PnpSignedDriver Get /Format:List (PID: 3064)

⚙️ 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
185.145.45.149 -> 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)



Retrive6218171138404779... WMIC.exe (1) ID.txt (2)

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

"xcopy "%PROGRAMFILES%\Java\jre1.8.0_25" "%APPDATA%\Oracle\" /e

%TEMP%\Retrive2420117266672210551.vbs

%TEMP%\Retrive2646804049303142888.vbs

%TEMP%\Retrive2670234531104625201.vbs

%TEMP%\Retrive3480961498146581831.vbs

%TEMP%\Retrive4681301751082619848.vbs

%TEMP%\Retrive6218171138404779966.vbs

%TEMP%\Retrive752908523483486178.vbs

%TEMP%\Retrive8824404834342482190.vbs

(Ljava/lang/String;)V
```

Extracted Files

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

Malicious 9

Retrive2420117266672210551.vbs

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Looking for file context ...

Size

276B (276 bytes)

Type

text

Description

ASCII text, with CRLF line terminators

AV Scan Result

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



SHA1	f92844fee69ef98db6e68931adfaa9a0a0f8ce66	
SHA256	9da575dd2d5b7c1e9bab8b51a16cde457b3371c6dcdb0537356cf1497fa868f6	

Retrive2646804049303142888.vbs

- Overview
- Download Disabled
- VirusTotal Report
- Metadefender Report
- Looking for file context ...

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: 312)

MD5	3bdfd33017806b85949b6faa7d4b98e4	
SHA1	f92844fee69ef98db6e68931adfaa9a0a0f8ce66	
SHA256	9da575dd2d5b7c1e9bab8b51a16cde457b3371c6dcdb0537356cf1497fa868f6	

Retrive2670234531104625201.vbs

- Overview
- Download Disabled
- VirusTotal Report
- Metadefender Report
- Looking for file context ...

Size 281B (281 bytes)
Type text
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

- Overview
- Download Disabled
- VirusTotal Report
- Metadefender Report
- Looking for file context ...

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: 300)



SHA256 45bfe34aa3ef932f75101246eb53d032f5e7cf6d1f5b4e495334955a255f32e7

Retrive4681301751082619848.vbs

Overview Download Disabled VirusTotal Report Metadefender Report Looking for file context ...

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 45bfe34aa3ef932f75101246eb53d032f5e7cf6d1f5b4e495334955a255f32e7

Retrive6218171138404779966.vbs

Overview Download Disabled VirusTotal Report Metadefender Report Looking for file context ...

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 Looking for file context ...

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



Retrive8824404834342482190.vbs

Overview

Download Disabled

VirusTotal Report

Metadefender Report

Looking for file context ...

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

Extended File Details

VirusTotal Report

Metadefender Report

Extracted Streams

Looking for file context ...

Size	46KiB (46592 bytes)
Type	peDll executable
Description	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
AV Scan Result	Labeled as "Trojan.Generic" (58/86)
Runtime Process	javaw.exe (PID: 2584)
MD5	0b7b52302c8c5df59d960dd97e3abdaf
SHA1	d85524f464dcded54edfcfe6a5056f6c4008bbcb
SHA256	a6be5be2d16a24430c795faa7ab7cc7826ed24d6d4bc74ad33da5c2ed0c793d0

Informative Selection

3

- _0.068614639798144752542616253131176441.class

▼
- _0.127476670696220488692148369551433214.class

▼
- GKPKtwfspIlg.ddKgDj

▼



Informative

2



ID.txt



test.txt



Notifications

Runtime



Community

Derek Knight commented 6 years ago

#java_adwind #jrat

! You must be logged in to submit a comment.

