

archer.dll

This report is generated from a file or URL submitted to this webservice on June 2nd 2017 17:56:11 (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 BeforeNo similar samplesReport False-PositiveRequest Report Deletion

malicious

Threat Score: 100/100

AV Detection: 75%

Labeled as: Bulz.Generic

#adware

- Post
- Link
- E-Mail

Incident Response

Indicators

- Malicious (4)
- Suspicious (9)
- Informative (10)

- File Details
- Screenshots (error)
- Hybrid Analysis (1)
- Network Analysis
- Extracted Strings
- Extracted Files (1)
- Notifications
- Community (0)

Back to top

Incident Response

	Risk Assessment
Persistence	Interacts with the primary disk partition (DR0)
Network Behavior	Contacts 1 domain and 1 host. <div>View all details</div>

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	
System Destruction	
Interacts with the primary disk partition (DR0)	
Hiding 1 Malicious Indicators	
All indicators are available only in the private webservice or standalone version	

Suspicious Indicators	9
Anti-Detection/Stealthyness	
Queries process information	
Environment Awareness	
Possibly tries to implement anti-virtualization techniques	
Queries physical drive (often used to detect virtual machines)	






























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

 HYBRID ANALYSIS	
 ▾	 ▾
	 ▾
	 ▾
	 Request Info ▾
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	

File Details

All Details: Off

archer.dll	
Filename	archer.dll
Size	139KiB (142336 bytes)
Type	pedll executable
Description	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

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](#)

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

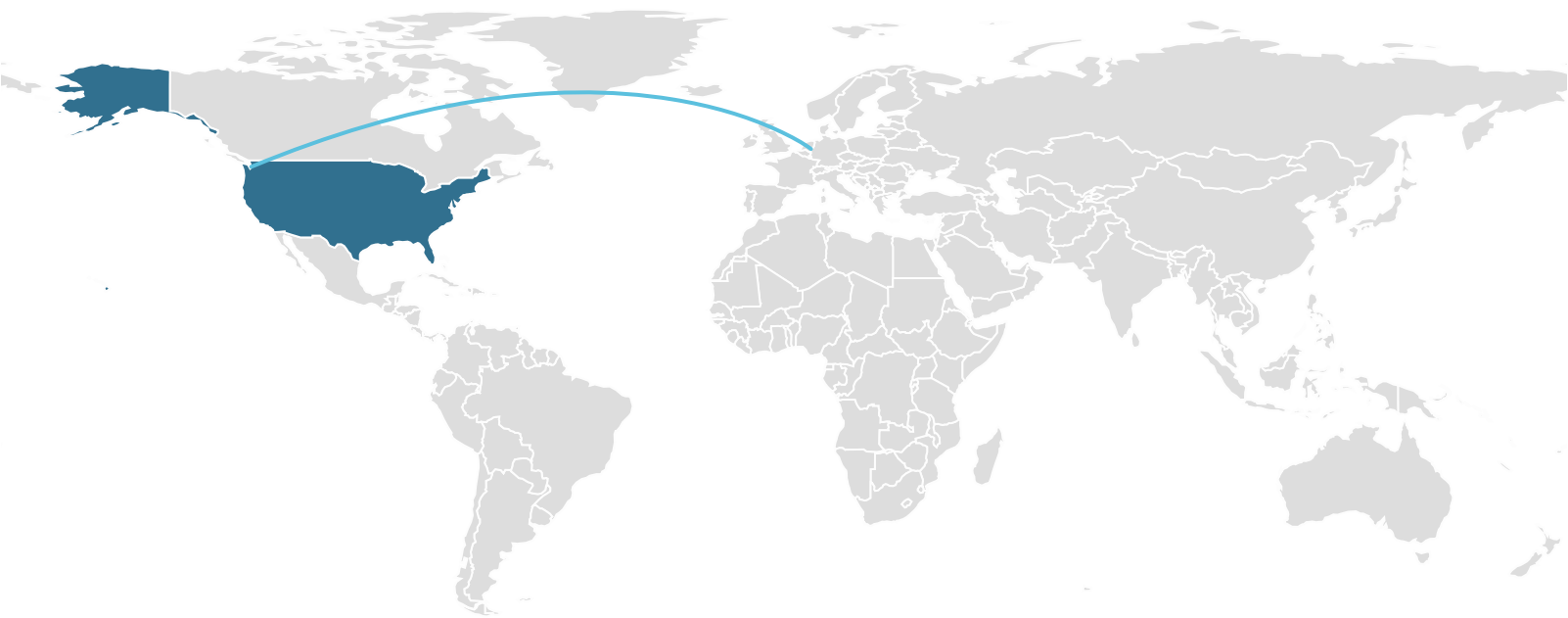
Domain	Address	Registrar	Country
dfrs12kz9qye2.cloudfront.net	54.230.216.113	-	United States

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
54.230.216.113 <div><div></div>OSINT</div>	80 TCP	rundll32.exe PID: 3308	United States ASN: 16509 (Amazon.com, Inc.)

Contacted Countries




HTTP Traffic

Endpoint	Request	URL	Data
54.230.216.113:80 (dfrs12kz9qye2.cloudfront.net)	GET	dfrs12kz9qye2.cloudfront.net//v4//sofclean//vboxxharddisk_vb47a275fd-833fcbf?action=actupd.0	GET //v4//sofclean//vboxxharddisk_vb47a275fd-833fcbf?action=actupd.0 HTTP/1.1 Host: dfrs12kz9qye2.cloudfront.net Cache-Control: no-cache <div></div> 200 OK <div><div></div>More Details</div>
54.230.216.113:80 (dfrs12kz9qye2.cloudfront.net)	GET	dfrs12kz9qye2.cloudfront.net//v4//sofclean//vboxxharddisk_vb47a275fd-833fcbf?action=actupd.2	GET //v4//sofclean//vboxxharddisk_vb47a275fd-833fcbf?action=actupd.2 HTTP/1.1 Host: dfrs12kz9qye2.cloudfront.net Cache-Control: no-cache <div></div> 200 OK <div><div></div>More Details</div>

Extracted Strings

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](#)

<div><div>HYBRID ANALYSIS</div><div><div><div></div><div></div><div></div><div></div><div></div></div><div>Request Info</div></div></div>
(((H
.?AV_Generic_error_category@std@@
.?AV_lostream_error_category@std@@
.?AV_System_error_category@std@@
.?AVbad_alloc@std@@
.?AVbad_exception@std@@
.?AVerror_category@std@@
.?AVexception@std@@
.?AVlength_error@std@@
.?AVlogic_error@std@@
.?AVout_of_range@std@@
.?AVtype_info@@

Extracted Files

Informative1

vboxxharddisk_vb47a275fd-833fcbff[1]

Overview

Download Disabled

Hash Seen Before

Size	3B (3 bytes)
Type	text
Description	ASCII text, with no line terminators
Runtime Process	rundll32.exe (PID: 3308)
MD5	4bb916da5a7ea9b96d7626fb84d59ab7
SHA1	76994171ab1079d196928aaca64e1d60f0d59769
SHA256	4f8ba43c1ee127eb3011f2b5fe3b754ceb566b000b558d252bbb4c87834de9a8

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](#)

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](#)