Joe Sandbox Cloud BASIC

ID: 562518
Sample Name: admin-ajax.php
Cookbook: default.jbs
Time: 23:57:52
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

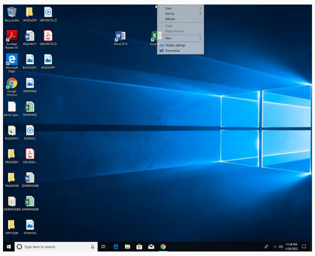
Windows Analysis Report

admin-ajax.php

Overview

General Information

Sample Name:	admin-ajax.php
Analysis ID:	562518
MD5:	156dca49797396..
SHA1:	bf05c18fd5813ce..
SHA256:	91392b0bfa15da..



Errors

- ⚠ No process behavior to analyse as no analysis process or sample was found
- ⚠ Corrupt sample or wrongly selected analyzer. Details: 80040153

Detection

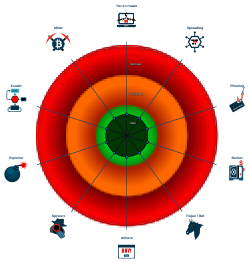
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Malware Configuration

⊘ **No configs have been found**

Yara Overview

⊘ **No yara matches**

Sigma Overview

⊘ **No Sigma rule has matched**

Jbx Signature Overview

There are no malicious signatures, click here to show all signatures.

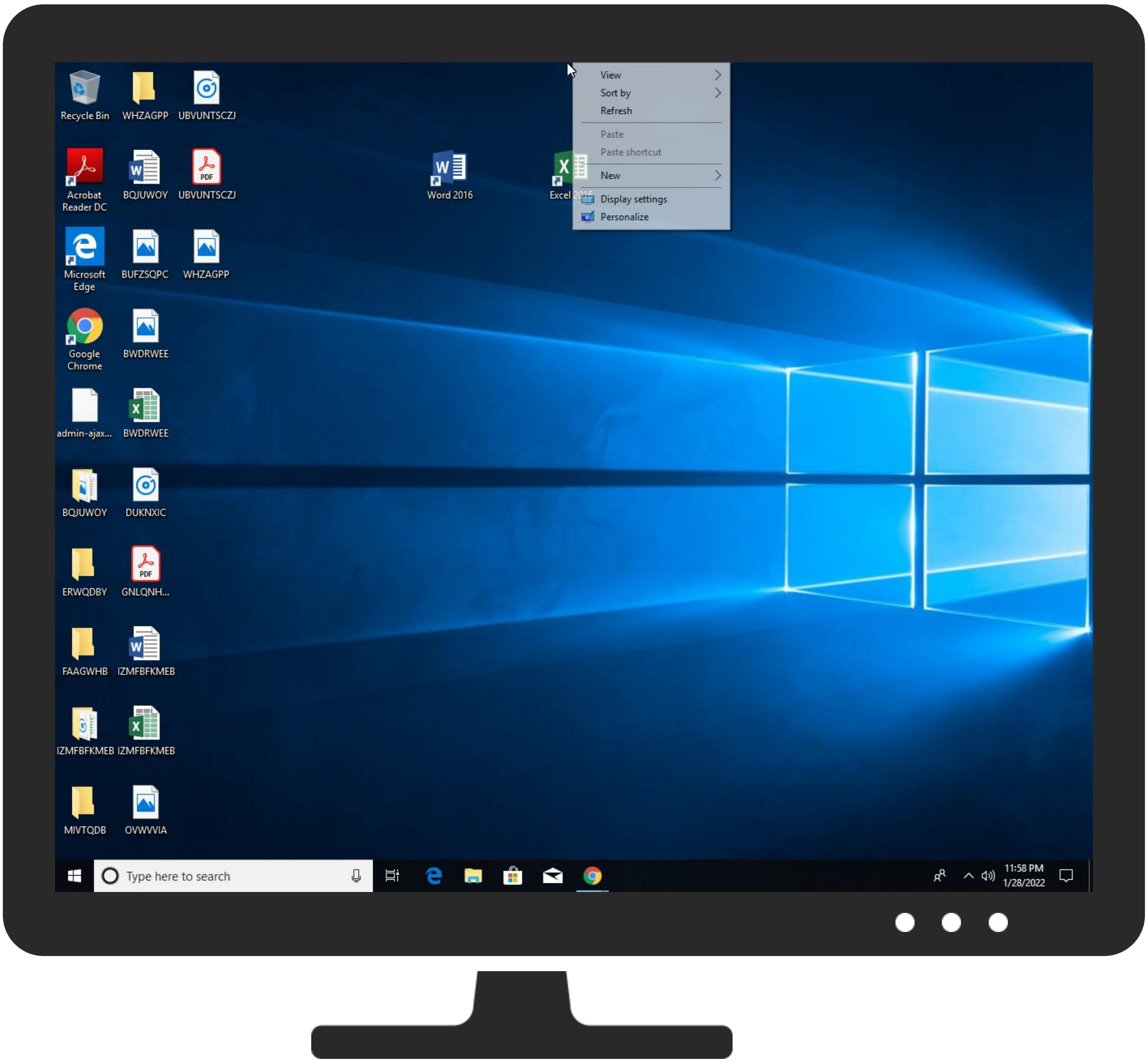
Mitre Att&ck Matrix

⊘ **No Mitre Att&ck techniques found**

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
admin-ajax.php	0%	Virustotal		Browse
admin-ajax.php	0%	Metadefender		Browse
admin-ajax.php	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
https://codex.wordpress.org/AJAX_in_Plugins	admin-ajax.php	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562518
Start date:	28.01.2022
Start time:	23:57:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	admin-ajax.php
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	1
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.winPHP@0/0@0/0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sample was found
- Corrupt sample or wrongly selected analyzer. Details: 80040153

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe
- Excluded IPs from analysis (whitelisted): 40.127.240.158, 20.49.150.241, 20.82.210.154
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com, settings-win.data.microsoft.com, arc.trafficmanager.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, arc.msn.com, settingsfd-geo.trafficmanager.net

Simulations

Behavior and APIs

⊘ **No simulations**

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

⊘ **No created / dropped files found**

Static File Info

General

File type:	PHP script, ASCII text
Entropy (8bit):	5.128729181822985

TrID:	
File name:	admin-ajax.php
File size:	4948
MD5:	156dca49797396866a8579a5ecd1a85f
SHA1:	bf05c18fd5813ce49f5741f870951de31ccbf3fa
SHA256:	91392b0bfa15da3a0ff06273d0dc891f85b33d73f09bcc187b94e36156ddb6dc
SHA512:	a3affdbf54ea38e060508efc3e7f4578d263390917c0b0ddc488b5be7c8c4b639e3e62c483d05cd287e61ccc129dc0ec258bc937c1ef4948acf77c23f6a38da5
SSDEEP:	96:0fmiivcJvoWdCKpVZn/i3sAqOkYKJceg4vCmXQP7mYfTPZm:0+pcqwCKRn/bOk3JfCT75E
File Content Preview:	<?php./**. * WordPress Ajax Process Execution. *. * @package WordPress. * @subpackage Administration. *. * @link https://codex.wordpress.org/AJAX_in_Plugins. */../* *. * Executing Ajax process.. *. * @since 2.1.0. */.define('DOING_AJAX', true);.if (! de

File Icon

Icon Hash:	74f0e4e4e4e4e0e4

Network Behavior

⊘ **No network behavior found**

Statistics

⊘ **No statistics**

System Behavior

⊘ **No system behavior**

Disassembly

⊘ **No disassembly**