

JOeSandbox Cloud **PRO**



**ID:** 4486943

**Cookbook:**

defaultwindowsinteractivecookbook.jbs

**Time:** 17:50:35

**Date:** 13/03/2025

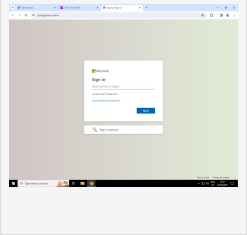
**Version:** 42.0.0 Malachite

# Windows Analysis Report

https://vawgcap-my.sharepoint.com/:o:/g/personal/andrew\_bennett\_vawg\_cap\_gov/EnVd5DcNv...

## Overview

### General Information

Sample URL:	https://vawgcap-my.sharepoint.com/:o:/g/personal/andrew_bennett_vawg_cap_gov...=5%3aQr9jJb&at=9&xsdata=MDV8MDJ8bWF0dC5zb2tVbG93QGhYXlUy29tIGRjZTRkYzQzNTR
Analysis ID:	4486943
Infos:	<div>Info</div>
	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Gabagool

Score:	76
Range:	0 - 100
Confidence:	100%

Signatures

Antivirus detection for URL or d...

Malicious sample detected (thro...

Yara detected Gabagool

HTML page contains hidden UR...

HTML page contains suspicious...

Phishing site detected (based o...

Form action URLs do not match...

HTML body contains low numbe...

HTML body with high number of...

HTML page contains hidden jav...

HTML title does not match URL

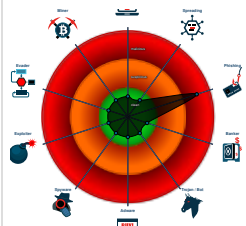
Javascript checks online IP of m...

Submit button contains javascr...

Uses Javascript AES encryption...

Yara signature match

Classification



## Signatures

### AV Detection

Antivirus detection for URL or domain

### Phishing

Yara detected Gabagool

HTML page contains hidden URLs

HTML page contains suspicious javascript code

Phishing site detected (based on logo match)

Form action URLs do not match main URL

HTML body contains low number of good links

HTML body with high number of embedded images detected

HTML page contains hidden javascript code

HTML title does not match URL

Javascript checks online IP of machine

Submit button contains javascript call

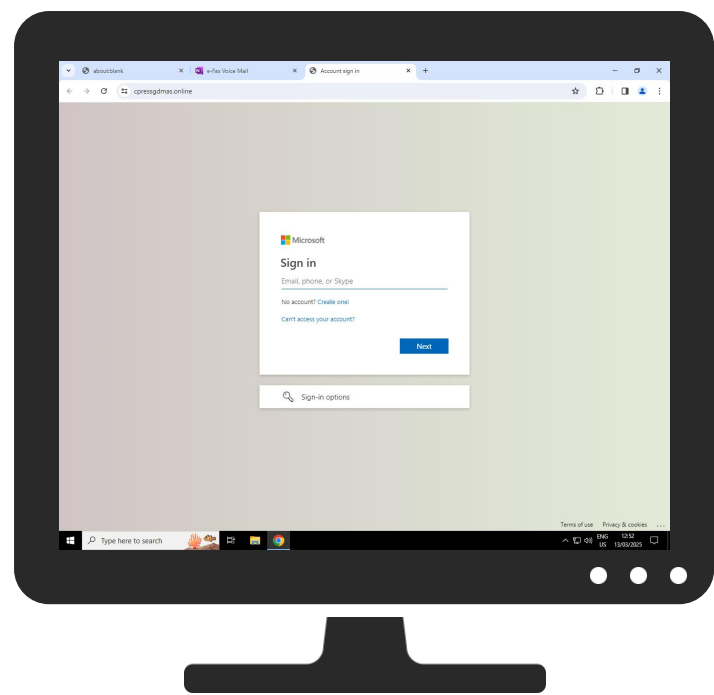
Uses Javascript AES encryption / decryption (likely to hide suspicious Javascript code)

### System Summary

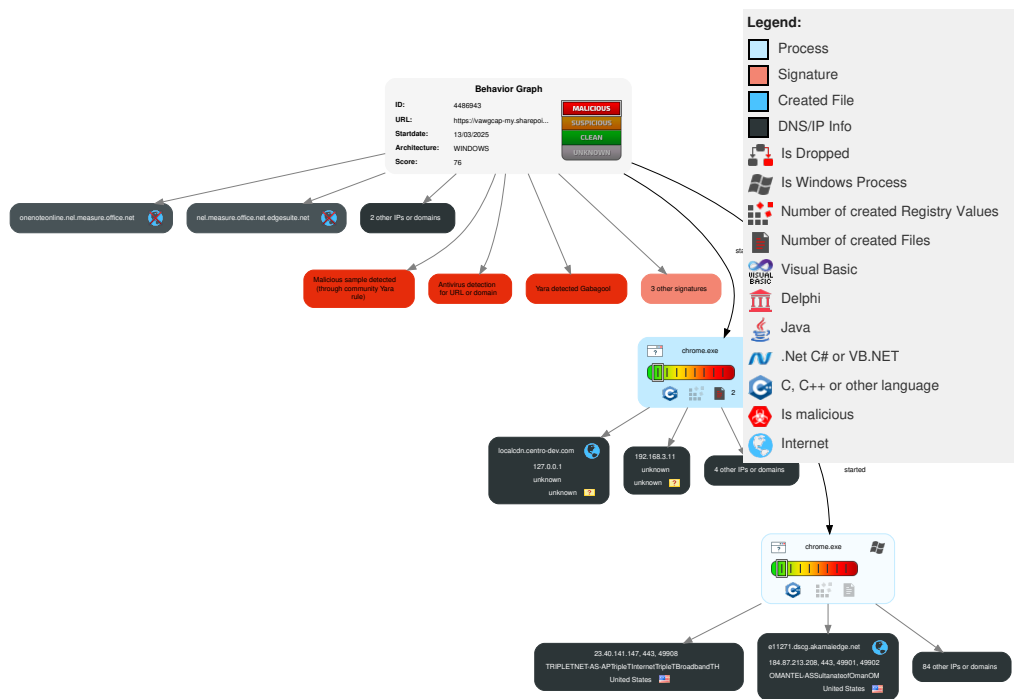
Malicious sample detected (through community Yara rule)

Yara signature match

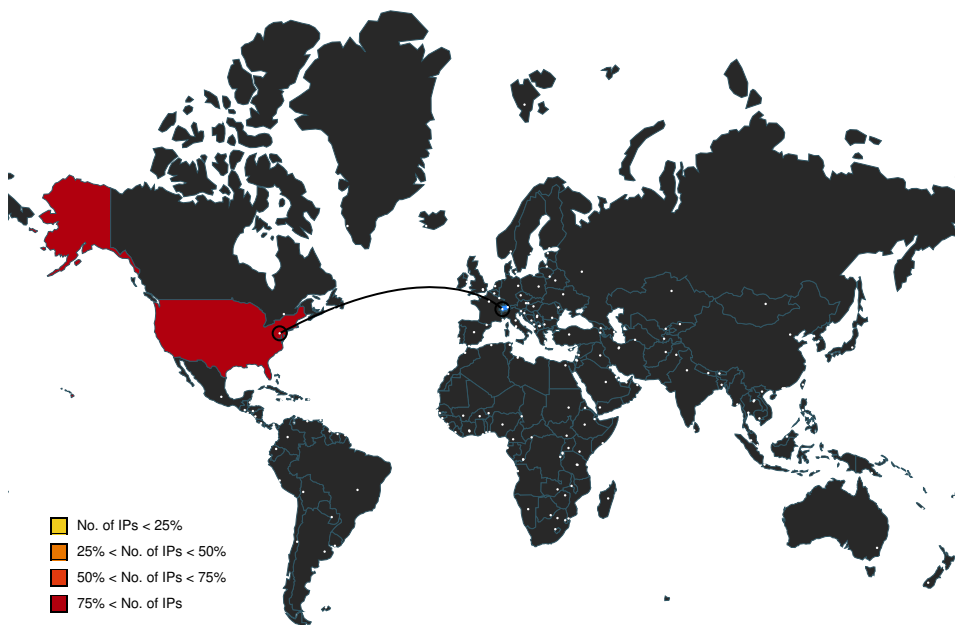
Screenshots




Behavior Graph









Network Map



#### Contacted Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.130.137	code.jquery.com	United States		54113	FASTLYUS	false
2.18.254.137	unknown	European Union		20940	AKAMAI-ASN1EU	false
23.40.141.147	unknown	United States		45758	TRIPLETNET-AS-APT TripleTInternetTripleT BroadbandTH	false
92.123.181.66	e329293.dscd.akamai-edge.net	European Union		20940	AKAMAI-ASN1EU	false
206.189.206.138	cpressgdmass.online	United States		14061	DIGITALOCEAN-ASNUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
2.19.192.98	unknown	European Union		20940	AKAMAI-ASN1EU	false
52.111.240.11	prod-campaignagggregator.o mexexternalfb.office.n et.akadns.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.21.27.207	wicked.bigpoliceman.com	United States		13335	CLOUDFLARENETUS	false
184.87.213.208	e11271.dscg.akamaiedge.net	United States		8529	OMANTEL-ASSultanateofOmanOM	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
2.19.192.66	a1531.g2.akamai.net	European Union		20940	AKAMAI-ASN1EU	false
13.107.136.10	dual-spo-0005.spo-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.190.177.23	www.tm.a.prd.aadg.trafficmanager.net	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
92.123.27.138	a46.dscr.akamai.net	European Union		16625	AKAMAI-ASUS	false
13.104.208.162	i-db3p-cor004.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.26.13.205	api.ipify.org	United States		13335	CLOUDFLARENETUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
52.111.231.2	augloop-prod-002.francecentral.cloudapp.azure.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.203.100	unknown	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
2.19.192.41	a1894.dscb.akamai.net	European Union		20940	AKAMAI-ASN1EU	false

#### Private

IP
192.168.3.11
127.0.0.1
192.168.3.4
192.168.3.5
192.168.3.2

## Contacted Domains

Name	IP	Active
dual-spo-0005.spo-msedge.net	13.107.136.10	true
i-db3p-cor004.api.p001.1drv.com	13.104.208.162	true
e329293.dscd.akamaiedge.net	92.123.181.66	true
a.nel.cloudflare.com	35.190.80.1	true
b-0004.b-msedge.net	13.107.6.156	true
a1894.dscb.akamai.net	2.19.192.41	true
augloop-prod-002.francecentral.cloudapp.azure.com	52.111.231.2	true
www.tm.a.prd.aadg.trafficmanager.net	20.190.177.23	true
cpressgdmaz.online	206.189.206.138	true
localcdn.centro-dev.com	127.0.0.1	true
a46.dscr.akamai.net	92.123.27.138	true
wac-0003.wac-msedge.net	52.108.8.12	true
prod-campaignagggregator.omexexternalfb.office.net.akadns.net	52.111.240.11	true
code.jquery.com	151.101.130.137	true
a726.dscd.akamai.net	23.41.187.16	true
cdnjs.cloudflare.com	104.17.24.14	true
wicked.bigpoliceman.com	104.21.27.207	true
www.google.com	172.217.168.36	true
a1531.g2.akamai.net	2.19.192.66	true
api.ipify.org	104.26.13.205	true
s-0005.dual-s-msedge.net	52.123.128.14	true
e11271.dscg.akamaiedge.net	184.87.213.208	true
s-part-0032.t-0009.t-msedge.net	13.107.246.60	true
js.monitor.azure.com	unknown	unknown
augloop.office.com	unknown	unknown
ajax.aspnetcdn.com	unknown	unknown
m365cdn.nel.measure.office.net	unknown	unknown
fa000000110.resources.office.net	unknown	unknown
onenoteonline.nel.measure.office.net	unknown	unknown
aadcdn.msauthimages.net	unknown	unknown
fa000000138.resources.office.net	unknown	unknown
amcdn.msftauth.net	unknown	unknown
www.onenote.com	unknown	unknown
messaging.engagement.office.com	unknown	unknown
fa000000096.resources.office.net	unknown	unknown
fa000000012.resources.office.net	unknown	unknown
fa000000111.resources.office.net	unknown	unknown
fa000000128.resources.office.net	unknown	unknown
aadcdn.msftauth.net	unknown	unknown
_5555_https.localcdn.centro-dev.com	unknown	unknown
storage.live.com	unknown	unknown
vawgcap-my.sharepoint.com	unknown	unknown
francecentral-002.augloop.office.com	unknown	unknown
common.online.office.com	unknown	unknown
login.microsoftonline.com	unknown	unknown
spoprod-a.akamaihd.net	unknown	unknown

## Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://m365cdn.nel.measure.office.net/api/report?FrontEnd=AkamaiCDNWorldWide&DestinationEndpoint=MILANO&ASN=20940&Country=IT&Region=&RequestIdentifier=0.16fddc17.1741884765.23e1f3ae&TotalRTCDNTTime=16&CompressionType=&FileSize=215	false		high
http://https://m365cdn.nel.measure.office.net/api/report?FrontEnd=AkamaiCDNWorldWide&DestinationEndpoint=MILANO&ASN=20940&Country=IT&Region=&RequestIdentifier=0.22fddc17.1741884766.5df93d0&TotalRTCDNTTime=15&CompressionType=&FileSize=215	false		high

