Jerusalem Post and other Israeli websites compromised by Iranian threat agent CopyKitten – ClearSky Cyber Security

Published: 2017-03-30 · Archived: 2026-04-29 07:11:46 UTC

On 29 March 2017 the German Federal Office for Information Security (BSI) said in a statement that the website of Israeli newspaper Jerusalem Post was manipulated and linked to a harmful third party. Below is a Google translation of the statement:

"After the cyber attack on the German Bundestag in 2015, some protective functions that the BSI has established for government networks have also been adopted by the German Bundestag for its own networks. ***Since the beginning of January 2017, the BSI, as the national cyber security agency, has been in close contact with the German Bundestag, due to the network traffic of the German Bundestag. At the request of the German Bundestag the BSI analyzed these problems in network traffic. The technical analyzes have been completed. The website of the Jerusalem Post was manipulated and linked to a harmful third party.*** *Within the framework of the analyzes, however, the BSI has not discovered any malicious software; infections are also not known to the BSI."*

As part of our monitoring of Iranian threat agents activities, we have detected that since October 2016 and until the end of January 2017, the Jerusalem Post, as well as multiple other Israeli websites and one website in the Palestinian Authority were compromised by Iranian threat agent CopyKittens. Based on the time-frame and nature of the compromises, we estimate with high certainty that the statement by German Federal Office for Information Security refers to the same incidents.

Watering hole attacks

In each of the compromised websites, the attackers inserted a single line of Javascript code into an existing Javascript library (a local library, loaded from the server hosting the compromised website). This code loaded further Javascript from a malicious domain owned by the attackers:

j**g**uery[.]net
Specifically from this URL: https://js.j**g**uery[.]net/jquery.min.js

Note that the domain is intentionally impersonating jquery.com, a legitimate and unrelated domain used by Jquery, one of the most prevalent Javascript libraries.

Below are screenshots of infected website's source code showing jguery[.]net being loaded (click images to enlarge).

Jerusalem post website (www.jpost.com):

Maariv – website of a national daily newspaper published in Israel (www.maariv.co.il)

The Israeli Defense Force Disabled Veterans Organization website (inz.org.il)

The Palestinian Ministry of Health (www.moh.gov.ps)

(loaded a from a similar malicious domain – jguery[.]online):

The student personal info log-in page of Tel Aviv University (www.ims.tau.ac.il)

This was captured by PassiveTotal as can be seen in the screenshot below or in the following analysis page: https://passivetotal.org/search/jguery.net.

By the time we examined the website the malicious code was removed.

Javascript payload

As can be seen in this public analysis, the malicious Javascript payload loaded from jguery[.]net and jguery[.]online was BeEF, The Browser Exploitation Framework Project, an open source "penetration testing tool that focuses on the web browser".

The Javascript payload was not served to each and every visitor of the infected websites. Based on our analysis and other indications, we estimate that the attackers used whitelisting, likely based on source IP. This means that only specific targets would be effected and potentially compromised. However, because we did not have access to the servers hosting the malicious Javascript payload, we do not know what was the exact logic for it being served.

Source of the compromise?

While monitoring online hacking communities, we identified that in October 2016 an actor sold access to the management panel of a server belonging to an Israeli hosting company. This server hosted the Jerusalem Post and Maariv, among other websites.

We estimate with medium certainty, that the attackers bought access to the server in order to deploy the malicious code.

Indicators of compromise

Indicators file: copykittens-indicators-March-2017.csv (also available on PassiveTotal).

Other parts of this campaign were revealed recently by Domaintools.

Domains in use by CopyKittens:

1e100[.]tech
1m100[.]tech
ads-youtube[.]online
akamaitechnology[.]com
alkamaihd[.]net
azurewebsites[.]tech
broadcast-microsoft[.]tech
chromeupdates[.]online
cloudmicrosoft[.]net
dnsserv[.]host
elasticbeanstalk[.]tech
fdgdsg[.]xyz
jguery[.]net
jguery[.]online
js[.]jguery[.]online
microsoft-ds[.]com
microsoft-security[.]host
nameserver[.]win
newsfeeds-microsoft[.]press
owa-microsoft[.]online
primeminister-goverment-techcenter[.]tech
qoldenlines[.]net
sharepoint-microsoft[.]co
ssl-gstatic[.]online
static[.]primeminister-goverment-techcenter[.]tech
trendmicro[.]tech
