CUJOAI

RAPID RESPONSE:

THE RISE OF SUSPICIOUS WEBSITES AT THE START OF THE ISRAEL-HAMAS WAR

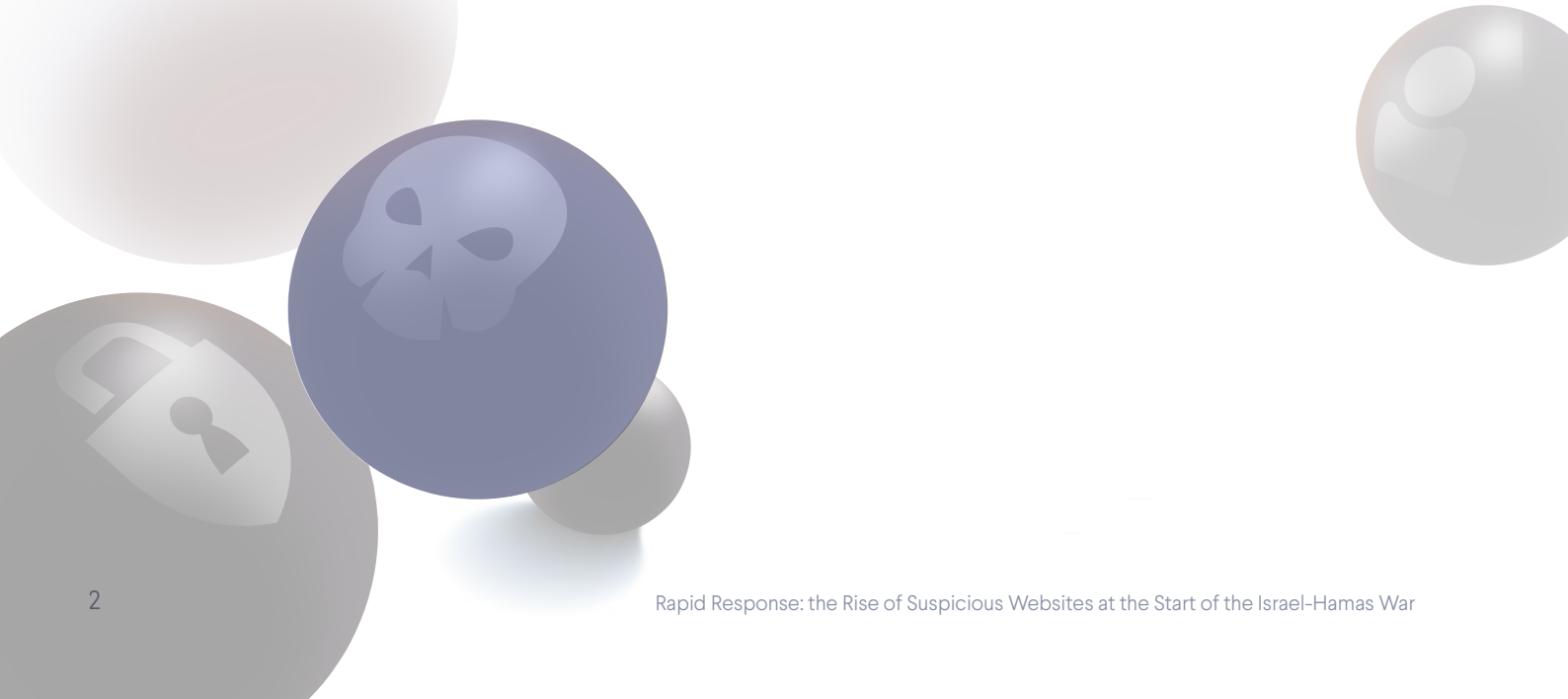
2024

Malicious actors often use events that draw the public's attention to promote scams. We have previously reported on the malicious activities targeting consumers during the COVID-19 pandemic and Russia's war against Ukraine. This year, we observed a similar spike in suspicious sites after the Hamas attack on Israel.

Malicious actors often use events that draw the public's attention to promote scams. We have previously reported on the malicious activities targeting consumers during the COVID-19 pandemic and Russia's war against Ukraine. This year, we observed a similar spike in suspicious sites after the Hamas attack on Israel.

In the aftermath of the October 7th attack, the number of visits to websites related to Israel, Palestine, Gaza, and Hamas increased three-fold. In an environment that garners a lot of support and drives donations, both legitimate and fraudulent websites can be set up within hours.

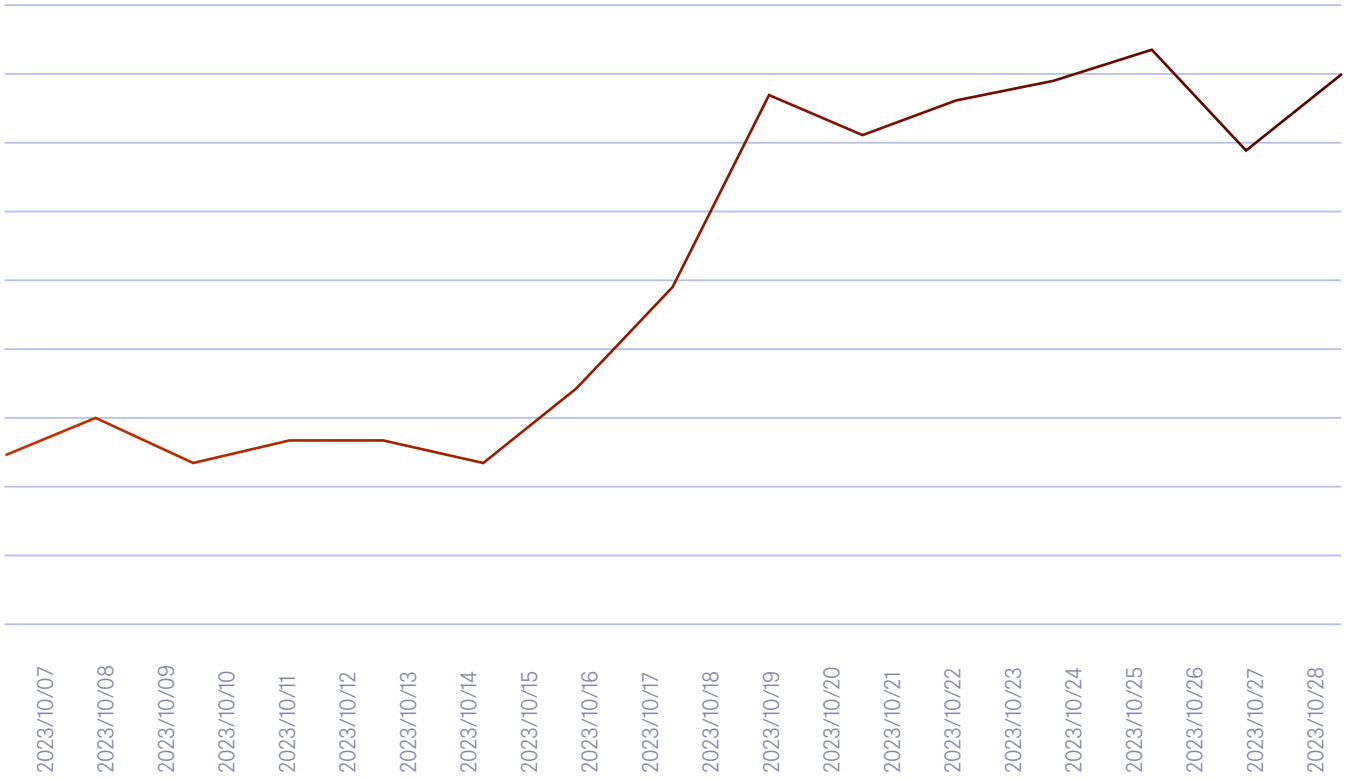
After the initial attack, the number of unique websites that mention support and donations to either Palestine or Israel continues to grow. In October, almost a third of these websites had new domains and asked for support in a suspicious manner.



Spike in Visits to Israel-Palestine Related Websites

Our data shows a three-fold (290% to 370%) increase in visits to websites related to charities, activist and support organizations in the week after October 7th.

SPIKE IN VISITS TO SITES RELATED TO SUPPORTING ISRAEL, PALESTINE, GAZA, OR HAMAS IN OCTOBER 2023

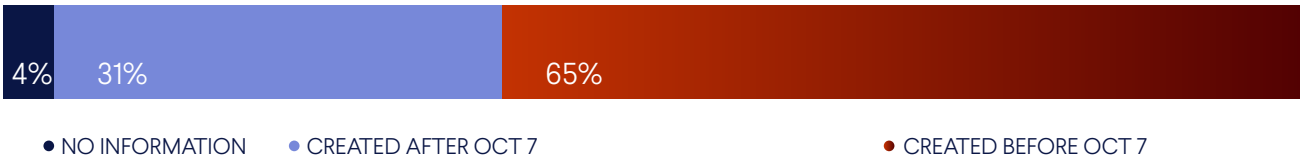


This data includes legitimate and suspicious websites and shows the scale of the interest that a shocking event can have. A highly engaged audience such as this is a convenient target for malicious actors: the urgency and willingness to get involved withhold is built in.

New Websites, Suspicious Websites

To have a better idea of how quickly the web reacts to such an event, we looked at when these websites had been registered. On October 22nd, **almost a third (30.9%) of all websites that users were visiting had been created after October 7th**.

DOMAIN CREATION DATE



NOTE: Data from 7-22 October.

Most (54.8%) of these new websites were **trying to attract donations**. Our researchers reviewed a large sample of these sites and noted that many were poorly designed and looked suspicious. As a rule, the most trustworthy sites were directing visitors to legitimate charities or non-profit organizations.

16% of the websites asked for donations in cryptocurrency, 7% sold t-shirts or other accessories as a form of donation. Around 10% of the websites had been started with page builders and were left unfinished.

A significant number (around 23%) of the new websites no longer existed on October 22nd, when this analysis started. These websites were either parked, suspended, not loading, or were redirecting visitors to unrelated websites. Our assumption here is that a significant number of these websites were fraudulent.

Zooming Out

We repeated our analysis in December to compare our findings with data from the initial analysis to see how the traffic dynamics and those new websites changed over time.

Overall, traffic to similar websites fluctuated around the new baseline that is three times larger than before the October 7th attack. In November, users visited a much wider range of domains (we saw three times as many domains being accessed between October 7–December 1 than between 7-22 October), but the number of domains registered after October 7th stayed roughly the same.

As a result, in early December, domains that were registered after October 7th made up just 12.6%.

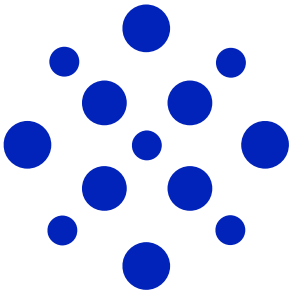
It is clear that the highest level of suspicious activity happened during the first week of the war, where the sense of urgency and ambiguousness was highest. Malicious actors jump to the opportunity to abuse painful experiences and scam good-willed people out of their money.

To protect people who do not evaluate the organizations they donate to, cybersecurity solutions have to rapidly detect and analyze new websites to alert users about suspicious sites almost instantly, since these sites may stay up.

Phishing Protection

CUJO AI Sentry is a multi-layer cybersecurity solution that offers Safe Browsing protection to protect every user on a network. Sentry works on the home network's router to stop connections to known malicious websites and uses our AI models to analyze previously unseen websites to protect consumers from phishing and other malicious websites. Sentry is deployed by some of the largest network operators in the world, and protects tens of millions of home networks, stopping over 8.000 threats every minute.

CUJO AI On The Move extends Safe Browsing protection for mobile devices outside the protected home network. Our data shows that malicious websites make up over 96% of all threats affecting mobile devices.



About CUJO AI Labs

CUJO AI Labs is an advanced research department of CUJO AI specializing in IoT threat research and NSP customer cybersecurity. Labs researchers use the largest scale real-world device behavior database of over 2 billion anonymized consumer devices to empower advanced machine learning technologies that protect tens of millions of households around the globe. Every year, CUJO AI Labs publishes in-depth data-based reports, such as this one, on the IoT ecosystem and cybersecurity.

About CUJO AI

CUJO AI provides advanced multilayered cybersecurity and device intelligence as a product for Internet Service Providers, which allow them to protect end users' devices and home networks.

Major mobile and broadband providers partner with CUJO AI to offer security as a value-added service to their clients.

As the only platform of its type deployed to in tens of millions of homes and covering over 2 billion connected devices, CUJO AI offers advanced AI algorithms to help its clients uncover previously unavailable insights and raise the bar on customer experience & retention with new value propositions and superior operational services.

Fully compliant with all privacy regulations, CUJO AI services are trusted by the largest broadband operators worldwide, including Comcast, Charter Communications, TELUS, Sky Italia, Rogers, Cox, Shaw, and Videotron.

More information: **connect@cujo.com**

Media inquiries: **press@cujo.com**

cujo.com