CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

October 19, 2023

Hamas Application Infrastructure Reveals Possible Overlap with TAG-63 and Iranian Threat Activity

Executive Summary

Insikt Group identified an application disseminated on a Telegram Channel used by members or supporters of the Hamas terrorist organization. The application is configured to communicate with Hamas's Izz ad-Din al-Qassam Brigades website — *alqassam[.]ps*. The website has worked intermittently since the start of Hamas's ground incursion into Israeli territory on October 7, 2023. From October 11, 2023, onward, we observed the domain point to multiple different IP addresses, which is likely related to attempts to evade website takedowns or, potentially, denial-of-service (DoS) attacks.

Infrastructure analysis associated with *alqassam[.]ps* led to the identification of a cluster of domains that mimic the domain registration tradecraft of TAG-63 (AridViper, APT-C-23, Desert Falcon), a cyber group that we believe operates at the behest of the Hamas terrorist organization. We also observed that these domains were interconnected via a Google Analytics code. The domains were also configured to redirect to *alqassam[.]ps*.

Last but not least, a domain associated with the cluster hosted a website that spoofs the World Organization Against Torture (OMCT). Again, based on domain registration patterns, we observed a likely Iran nexus tied to that domain.

Recorded Future Network Intelligence revealed a significant uptick in network traffic to the IP addresses hosting *alqassam[.]ps,* which overlapped with the start of Hamas's attack on October 7, 2023, as well as a significant reduction in traffic by late on October 10 (all times in this report are in UTC). This is potentially due to website outages or denial-of-service (DoS) attacks directed at the website by third parties.

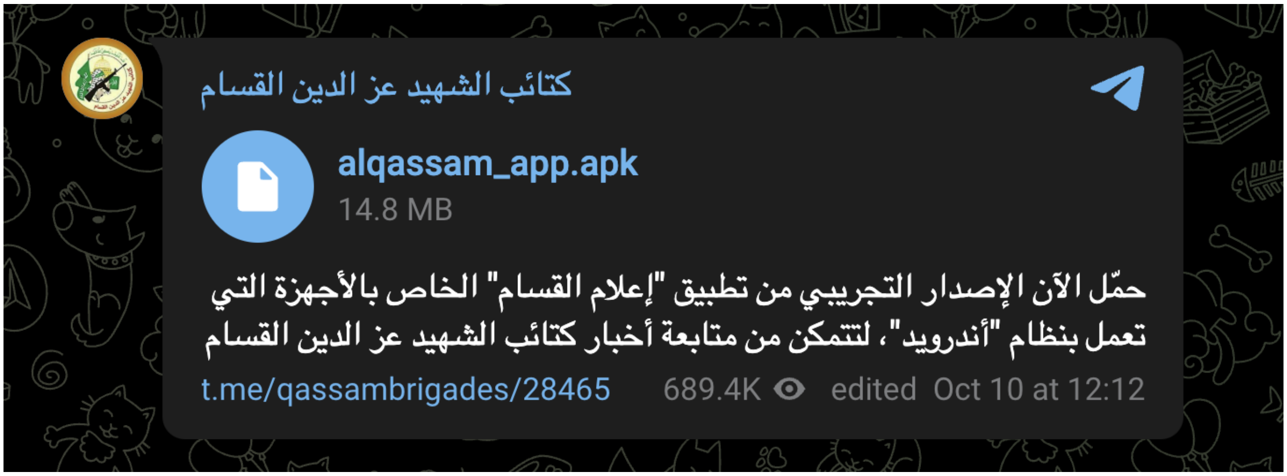
Key Findings

- The application dropped in a Telegram Channel claiming affiliation to Hamas's Izz ad-Din al-Qassam Brigades was designed to enhance the dissemination of the organization's message via that application.
- Multiple domains identified through Insikt Group infrastructure research revealed that they shared a specific Google Analytics code; various domains were also identified redirecting to the Izz ad-Din al-Qassam Brigades website.
- We observed domain registration tradecraft commonly associated with TAG-63, which shared the website redirect to the Izz ad-Din al-Qassam Brigades website.
- Our analysis suggests that infrastructure likely operated by the same threat actors revealed an Iran nexus based on subdomain naming registration conventions. One of the subdomains associated with this cluster hosted a spoofed page associated with the World Organization Against Torture.
- Recorded Future Network Intelligence observed an influx of network traffic to IP addresses hosting the Izz ad-Din al-Qassam Brigades website at the start of Hamas's incursion into Israeli territory on October 7, 2023.

Analysis

The Al Qassam Application

The Al Qassam application was posted on October 10, 2023, via a Telegram Channel[1] called "كتائب الشهيد عز الدين القسام" (Martyr Izz ad-Din al-Qassam Brigades) (**Figure 1**), where it was disseminated to be shared with the group's membership base.



كتائب الشهيد عز الدين القسام

alqassam_app.apk
14.8 MB

حمّل الآن الإصدار التجريبي من تطبيق "إعلام القسام" الخاص بالأجهزة التي
تعمل بنظام "أندرويد"، لتتمكن من متابعة أخبار كتائب الشهيد عز الدين القسام

t.me/qassambrigades/28465 689.4K edited Oct 10 at 12:12

***Figure 1**: The application was advertised on the Telegram Channel of the Qassam Brigade on October 10, 2023. The statement reads: "Download now the trial version of the 'Al-Qassam Media' application for 'Android' devices, so you can follow the news of the Martyr Izz al-Din al-Qassam Brigades". (Source: Telegram)*

The application is configured to communicate with the domain that acts as an outlet for the Qassam Brigade — *alqassam[.]ps* — which, at the time of this analysis, resolved to the IP address *5.45.81[.]22* and is owned by a Panamanian entity called "IROKO Networks Corporation" (AS12722). We observed the domain point to multiple different IP addresses from October 11, 2023, onward (**Table 1**).

[1] https[:]//t[.]me/qassambrigades/28465

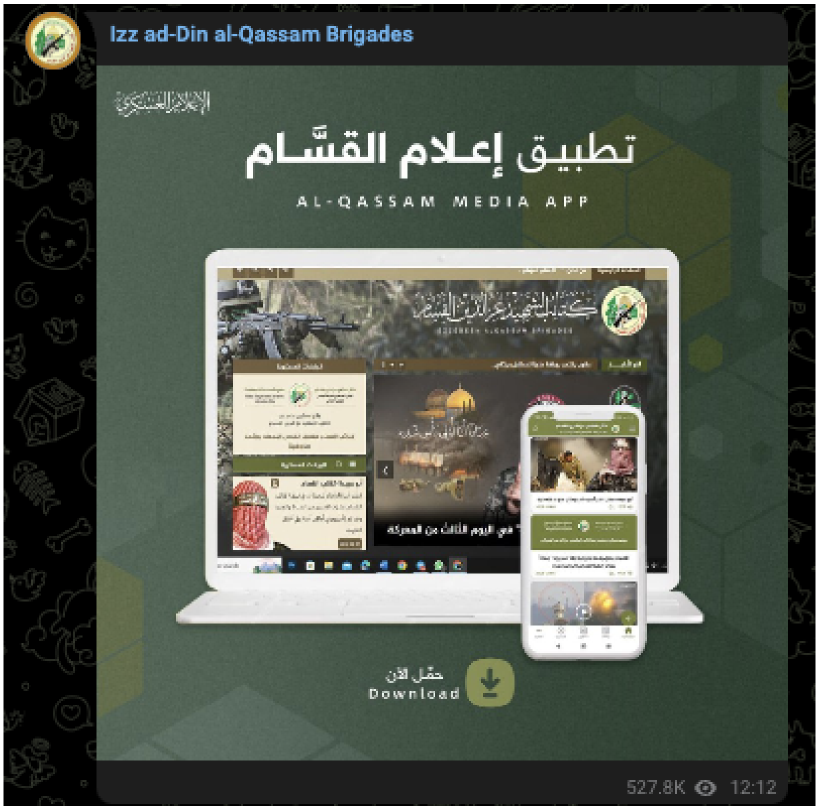


Figure 2*: The application has direct links to the website of the Hamas organization (Source: Telegram)*

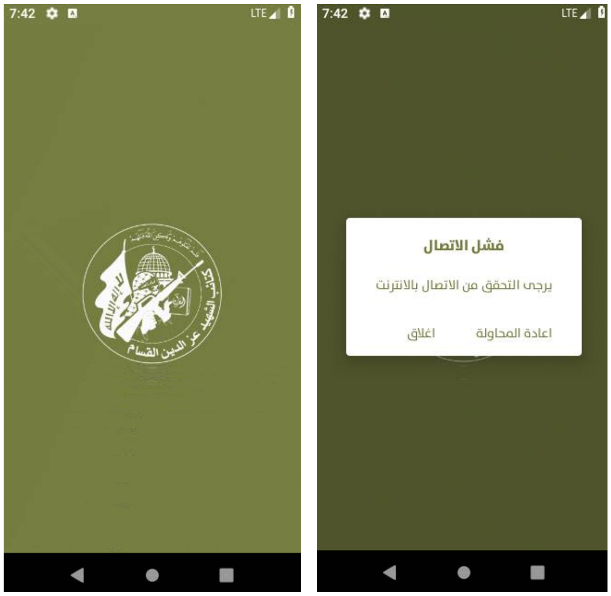
The domain — *alqassam[.]ps* — resolved to *176.114.6[.]214* from May 2021 until October 11, 2023. On October 11, the domain changed its resolution to *185.209.31[.]193*, an IP address owned by a Russian entity, "VDSINA VDS Hosting" (AS48282). According to public reports, this ASN is associated with "Hosting Technology LTD'', an entity located in Moscow, Russia.

Domain	IP Address	ASN	Registrar	WHOIS Data	First Seen	Last Seen
alqassam[.]ps	5.45.81[.]22	IROKO Networks Corporation (Panama) (AS12722)	"Maktab"	ahmed.alqassam@gmail[.]com omar_mano@msn[.]com "Ehab Ahmad" "Mohammed"	10-15-2023	10-17-2023
	45.142.137[.]107	Energy Bridge Sarl (Lebanon) (AS56902)			10-16-2023	10-17-2023
	85.202.95[.]107	Khodor Kanso Access Lebanon (Lebanon) (AS199239)			10-15-2023	10-16-2023
	185.209.31[.]193	Hosting Technology LTD (Russia) (AS48282)			10-11-2023	10-14-2023
	176.114.6[.]214	Oleksandr Siedinkin (Ukraine) (AS56485)			05-28-2021	10-11-2023

Table 1: *pDNS resolutions associated with the Hamas application infrastructure (Source: Recorded Future and DomainTools)*

Sandbox Analysis

When analyzed in Recorded Future's sandbox (Android emulator), the application installed and successfully launched but failed to load content, claiming a "connection failure" as noted in **Figure 3**. The 2 options below the "connection failure" notification enable the user to attempt to connect again via the "Try Again" (اعادة المحاولة) option; we tried via various instances of the application loaded on different virtual machines, but it failed to load content. The other option, "Close" (اغلاق), allows a user to cancel, at which point the application terminates. As of this writing, it is almost certain the application was not able to communicate successfully with the host website as it was knocked offline, potentially due to hacktivist operations or a hosting provider takedown.



فشل الاتصال

يرجى التحقق من الاتصال بالانترنت

***Figure 3**: (Left) The application's interface when it loads in an Android environment; (Right) "Connection Failure" notification (Source: [Recorded Future](#))*

The application has been identified via different name variants (**Table 2**), but as of this writing all known files are configured to communicate with *alqassam[.]ps.* Both the Recorded Future sandbox and [third-party](#) sandboxes have determined the Android version of the application to be suspicious. That said, the application does not request access to sensitive information from the device (such as images, access to microphones and cameras, SMS, or geolocation data).

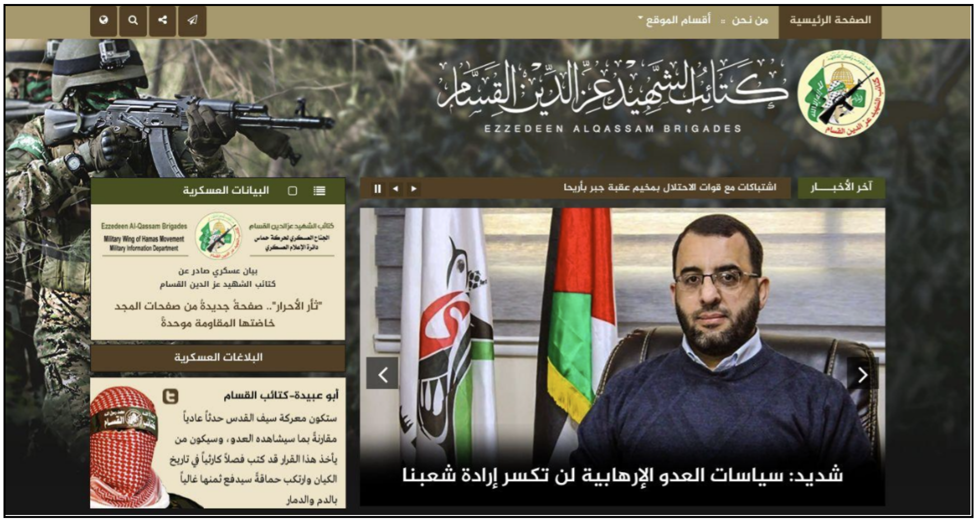
SHA256 Hash File Name	File Name	Creation Timestamp	First Seen (Analysis)
04880196c8927d7fcaf32d6cc55f5b7a33858f65de70a968efc0ea8d9f7221c2	alqassam_app.apk	01-01-1981	10-10-2023
	Kasman_1001.apk		
	198972		

***Table 2:** Application names identified in the wild (Source: [VirusTotal](#))*

Infrastructure Pivots

Identification of Domains and Suspected Link to TAG-63

We identified a cluster of domains that share the Google Analytics code *UA-53251638*, which is associated with domains linked to Hamas threat actors, including the Al Qassam website (**Tables 3 and 4**). 4 of the 5 domains match the domain registration convention of TAG-63 domains we have identified as part of our threat tracking. The domains listed in **Tables 3 and 4** all shared the same redirect to *alqassam[.]ps.*


الصفحة الرئيسية
من نحن
أقسام الموقع
كتائب الشهيد عز الدين القسام
EZZEDEEN ALQASSAM BRIGADES
آخر الأخبـــار
البيانات العسكرية
Ezzedeen Al-Qassam Brigades
Military Wing of Hamas Movement
Military Information Department
كتائب الشهيد عزالدين القسام
الجناح العسكري لحركة حماس
دائرة الإعلام العسكري
البلاغات العسكرية
أبو عبيدة-كتائب القسام

اشتباكات مع قوات الاحتلال بمخيم عقبة جبر بأريحا

بيان عسكري صادر عن
كتائب الشهيد عز الدين القسام

"ثأر الأحرار".. صفحةٌ جديدةٌ من صفحات المجد
خاضتها المقاومة موحدةً

ستكون معركة سيف القدس حدثاً عادياً مقارنةً بما سيشاهده العدو، وسيكون من يأخذ هذا القرار قد كتب فصلاً كارثياً في تاريخ الكيان وارتكب حماقةً سيدفع ثمنها غالياً بالدم والدمار

شديد: سياسات العدو الإرهابية لن تكسر إرادة شعبنا

Figure 4: *Website redirect for the domains identified in Table 2 to the Qassam Brigades outlet (Source: DomainTools)*

TAG-63 domains typically use English-language names — such as *beatricewarner[.]com* or *criston-cole[.]com* — and are linked to attack activity through the dissemination of Micropsia malware. In this case, the domains were all registered using the `.icu` top-level domain (TLD) and, unlike the Hamas website, used privacy protections to mask the registrant name and other WHOIS data. The threat actors also employed CloudFlare content distribution network (CDN) services for all domains after they were registered using the NameCheap domain registration and hosting provider. Based on the overlapping indicators, including the time of registration, we assess the domains are almost certainly managed by Hamas operators.

Domain	IP Address First Resolved	ASN	Registrar	First Seen (UTC)
isabeljwade[.]icu	198.54.117[.]210[2]	AS22612	NameCheap	04-27-2023 9:20 AM
francescatmorrison[.]icu	198.54.117[.]210	AS22612	NameCheap	04-27-2023 9:20 AM
jayyburrows[.]icu	198.54.117[.]210	AS22612	NameCheap	04-27-2023 9:20 AM
jessicakphillips[.]icu	198.54.117[.]210	AS22612	NameCheap	04-27-2023 9:20 AM

Table 3: *Newly identified domains matching TAG-63 domain registration tradecraft linked to the Qassam Brigades websites (Source: Recorded Future and DomainTools)*

[2] This IP address is hosting legitimate domains and should not be assessed as attacker-controlled infrastructure. This IP address is linked to the TAG-63 domains, however, via "First Seen" domain registration data.

The domains listed in **Table 3** are listed as malicious (1, 2, 3, 4) by a small number of antivirus engines; Insikt Group has not identified any samples pointing to a specific malware family, like Micropsia.

Infrastructure Link to Iran

We observed a final domain — *nikanps[.]top* — sharing the above-noted redirect to the Al Qassam Brigades website on May 25, 2023. This domain's registration history and details were also different from the domains listed in **Table 3**. The domain *nikanps[.]top* was first registered on May 9, 2023, and resolved to the Hetzner Online GmbH IP address as depicted in **Table 4**. The registrant also used privacy protections to mask all pertinent WHOIS data. At the time of writing, the domain is not listed as malicious by antivirus engines.

Domain	IP Address First Resolved	ASN	Registrar	First Seen
nikanps[.]top	91.107.188[.]236	AS24940	CSL Computer Service Langenbach GmbH	05-09-2023 1:59 AM

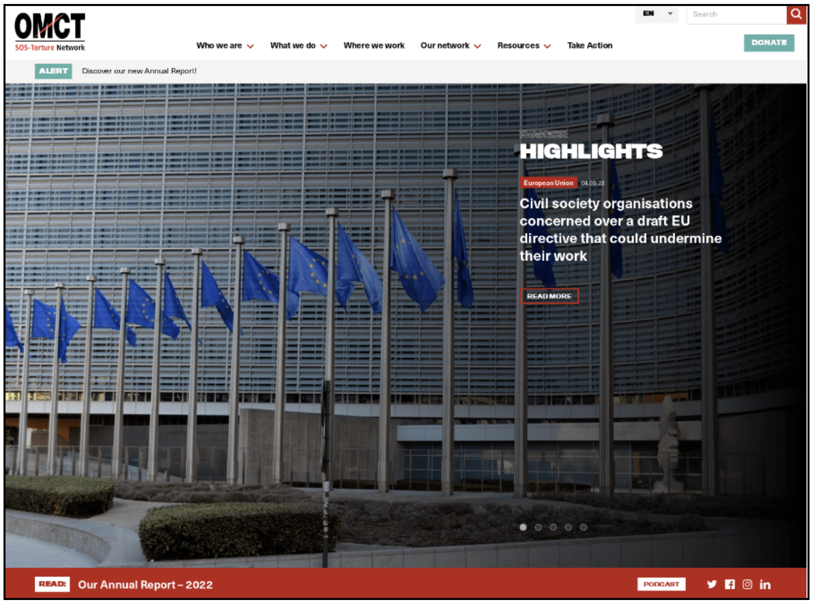
Table 4: *Domain sharing link to Qassam Brigades website and the suspected spoofing of the OMCT (Source: Recorded Future and DomainTools)*

Recorded Future pDNS data indicates that the domain owner is highly likely also responsible for registering the Dynamic DNS (DDNS) domain *nikanpsx.hopto[.]org* , which resolved to the same IP address (*91.107.188[.]236*) in May 2023. As of this writing, the DDNS domain has not been listed as malicious by antivirus engines.

Various subdomains of *nikanps[.]top* shared naming links to Iran, such as *iran.nikanps[.]top* , *hamrah.nikanps[.]top* , and *modir.nikanps.top* , for example. In Farsi, the terms "hamrah" and "modir" mean "attendant" (or "along" or "comrade"), and "director" (or "manager"), respectively. As of this writing, we have not been able to determine how they have been used by the owners of the domains.

The OMCT Page

The *nikanps[.]top* domain was, however, used to spoof a landing page associated with the World Organization Against Torture (OMCT) (**Figure 5**). A subdomain — *user.nikanps[.]top* — that pointed to 2 IP addresses from May 9 to May 11, 2023, was detected via a urlscan submission on May 9.



Civil society organisations concerned over a draft EU directive that could undermine their work

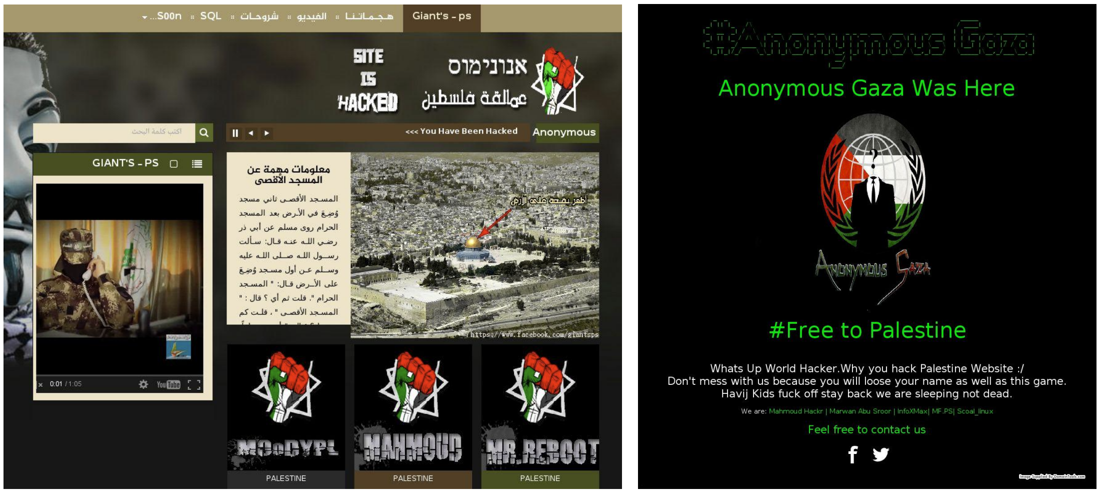
Figure 5*: Subdomain user.nikanps[.]top hosted a page spoofing the World Organization Against Torture (Source: urlscan)*

At the time of submission, the subdomain resolved to *91.107.129[.]43*. The second IP address that hosted *user.nikanps[.]top* was *91.107.188[.]236*, and while multiple other domains were hosted on the latter IP address, only 2 others pointed to the former: *admin.nikanps[.]top* and *hz.nikanpsx[.]top*. The earliest known "A" record of *hz.nikanpsx[.]top* dates to early January 2023. As of this writing, we have not identified any malicious activity associated with the domain or infrastructure.

It is highly likely that the *nikanpsx[.]top* domain is owned by the same threat actors responsible for the DDNS domain — *nikanpsx.hopto[.]org* — as well as *nikanps[.]top*. We have observed notable hosting overlaps between subdomains associated with both apex domains — *nikanpsx[.]top* and *nikanps[.]top* — since January 2023.

Google Code and Links to Palestinian Hacktivist Operations

We observed that many of the domains that share the same Google Analytics code (*UA-53251638*) were also compromised and defaced (these are historical records) by threat actors that support the Gaza-based organization behind the domain. In one of the defacements depicted in **Figure 6**, a compromised Israeli website is defaced by an entity claiming to be Giant's-PS, a known hacktivist group affiliated with the Palestinian Territories. One of the defacements revealed an uploaded video of an operative dressed in military fatigues, with the Al Qassam Brigades flag in the background. We note, however, that not all websites observed to have been defaced shared the same messaging and presumed allegiance to the Qassam Brigades, as some depicted general support for Palestinian statehood.



معلومات مهمة عن المسجد الأقصى

المسجد الأقصى ثاني مسجد وُضِعَ في الأرض بعد المسجد الحرام روى مسلم عن أبي ذر رضي الله عنه قال: سألت رسول الله صلى الله عليه وسلم عن أول مسجد وُضِعَ على الأرض قال: " المسجد الحرام ". قلت ثم أي ؟ قال : " المسجد الأقصى "، قلت كم

Anonymous Gaza Was Here

#Free to Palestine

Whats Up World Hacker.Why you hack Palestine Website :/
Don't mess with us because you will loose your name as well as this game.
Havij Kids fuck off stay back we are sleeping not dead.

We are: Mahmoud Hackr | Marwan Abu Sroor | InfoXMax| MF.PS| Scoal_linux

Feel free to contact us

Figure 6*: (Left) Qassam Brigades flag observed in the background of an uploaded video to the compromised website; (Right) Anonymous Gaza defacement page (Source: DomainTools)*

Network Intelligence

Recorded Future Network Intelligence revealed an increased level of traffic to *alqassam[.]ps* and associated IP addresses that we investigated, which overlapped with the start of the ground attack into Israeli territory on October 7, 2023. The sustained traffic peaked and started to decline by October 10. We observed expected network traffic to a website that included connections to ports 80 and 443 from globally dispersed IP addresses.

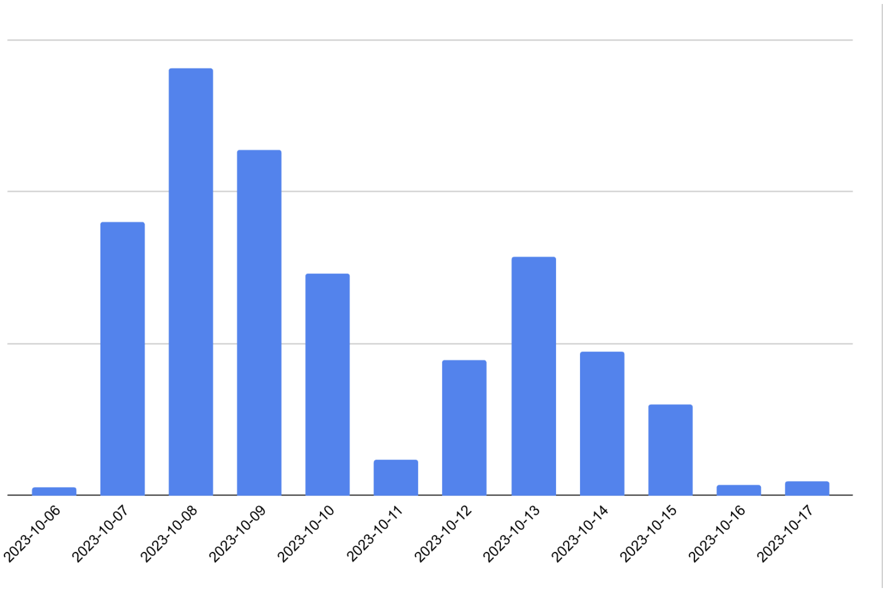


Figure 7*: Visualization of network communications to IP addresses hosting alqassam[.]ps (Source: Recorded Future)*

The observation could be explained as internet user navigation to the organization's website, likely by supporters or parties seeking to acquire information about the group's activities, as information was shared by the group. Another explanation could be that the increased traffic may have been caused by third parties seeking to attack the website using DoS techniques.

Outlook

The infrastructure overlaps that were identified between the Hamas application and the cluster of domains we suspect are linked to TAG-63 tradecraft are notable — they depict not only a possible slip in operational security but also ownership of the infrastructure shared between groups. One possible hypothesis to explain this observation is that TAG-63 shares infrastructure resources with the rest of the Hamas organization.

In relation to the Iran-nexus infrastructure link, we assess it is likely that the newly identified domains (*nikanps[.]top* and *nikanpsx[.]top*) were operated by threat actors that share an organizational or ideological affiliation with the Qassam Brigades. At the time of writing, Iran's Islamic Revolutionary Guard Corps (IRGC), and specifically the Quds Force, is the only known entity from Iran that provides cyber technical assistance to Hamas and other Palestinian threat groups.

Appendix A — Indicators[3]

Domains:
```
alqassam[.]ps
nikanps[.]top
hamrah.nikanps[.]top
modir.nikanps.top
admin.nikanps[.]top
user.nikanps[.]top
nikanpsx[.]top
hz.nikanpsx[.]top
nikanpsx.hopto[.]org
isabeljwade[.]icu
francescatmorrison[.]icu
jayyburrows[.]icu
jessicakphillips[.]icu
```

IP addresses:
```
185.209.31[.]193
176.114.6[.]214
91.107.188[.]236
91.107.129[.]43
198.54.117[.]210
5.45.81[.]22
```

Application SHA256 Hash:
```
04880196c8927d7fcaf32d6cc55f5b7a33858f65de70a968efc0ea8d9f7221c2
```

[3] Please note that this infrastructure is not entirely reflective of malicious attacker controlled infrastructure. In some instances, such as with 198.54.117[.]210 the infrastructure highlighted was purely to indicate a "First Seen" record. Researchers should evaluate each indicator for malicious activity within their networks.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com.