

The Hactivist Response to UK Foreign Policy

 cyjax.com/the-hactivist-response-to-uk-foreign-policy/

2 September 2024

Introduction

Hactivism is by its very nature reactive, as it involves the use of computer-based techniques as a form of civil disobedience to promote a political agenda or social change. Groups conduct attacks in response to the actions of others, both to encourage or discourage these actions. With the emergence and developments of the Russia-Ukraine war and the Israel-Palestine conflict escalations, there has been a resurgence in hactivism over the past few years. As different countries, including the United Kingdom, orientate themselves to supporting various belligerents, many new groups have formed, new techniques have been adopted, and the space has shifted significantly to one that is almost unrecognisable when compared to the previous decade. Hactivist groups can often be found on social media platforms, with Telegram being the most prominent place of operations. The actions of various nations during the aforementioned conflicts have been a frequent trigger for hactivist activity. In this blog, Cyjax will explore how the various players have responded to recent reporting of significant geopolitical developments in the United Kingdom as it supports Ukraine and strategic allies in the Middle East.

Attack claims

A common attack method hactivist groups employ is Distributed Denial-of-Service (DDoS) attacks. These are a method of disruption where a threat actor uses multiple devices, usually in quantities of hundreds to thousands, to send large amounts of traffic to a targeted server simultaneously and cause outages. CheckHost tracks outage reports and displays them graphically for a specified time period. When claiming responsibility for successful DDoS attacks, hactivists often share CheckHost reports which show the downtime experienced by the target during a given time in an effort to provide some legitimacy to their claims. However, through corresponding CheckHost reports do not legitimise a DDoS attack claim by itself, they do provide circumstantial evidence that an attack likely occurred.

Check website https://mydup.com/				
Permanent link to this check report Share on Twitter				Live server terminal
Checked on Thu Jul 04 17:48:14 UTC 2024 Check again				
Location ▾	Result	Time	Code	IP address
Brazil, Sao Paulo	Server error	22.083 s	503 (Service Unavailable)	172.67.152.228
Bulgaria, Sofia	Too many open files			
Croatia, Sisak	Server error	14.377 s	503 (Service Unavailable)	188.114.97.11
Czechia, C.Budejovice	Server error	4.204 s	502 (Bad Gateway)	172.67.152.228
Finland, Helsinki	Server error	22.410 s	503 (Service Unavailable)	104.21.2.203
France, Paris	Server error	10.118 s	504 (Gateway Time-out)	188.114.97.2
Germany, Frankfurt	Server error	10.122 s	504 (Gateway Time-out)	188.114.97.3
Germany, Nuremberg	Server error	4.293 s	502 (Bad Gateway)	188.114.96.3
Hong Kong, Hong Kong	Server error	11.095 s	504 (Gateway Time-out)	104.21.2.203
India, Mumbai	Server error	10.895 s	504 (Gateway Time-out)	104.21.2.203
Iran, Esfahan	Server error	11.076 s	504 (Gateway Time-out)	188.114.96.6
Iran, Karaj	Server error	4.134 s	502 (Bad Gateway)	104.21.2.203
Iran, Shiraz	Server error	14.808 s	503 (Service Unavailable)	188.114.96.6
Iran, Tehran	Server error	3.950 s	502 (Bad Gateway)	188.114.96.3
Israel, Netanya	Server error	4.146 s	502 (Bad Gateway)	188.114.96.7
Israel, Tel Aviv	Server error	4.129 s	502 (Bad Gateway)	188.114.97.7

Figure 1. Checkhost report showing outage against the website of the UK's Democratic Unionist Party (DUP)

Attacks conducted against the UK

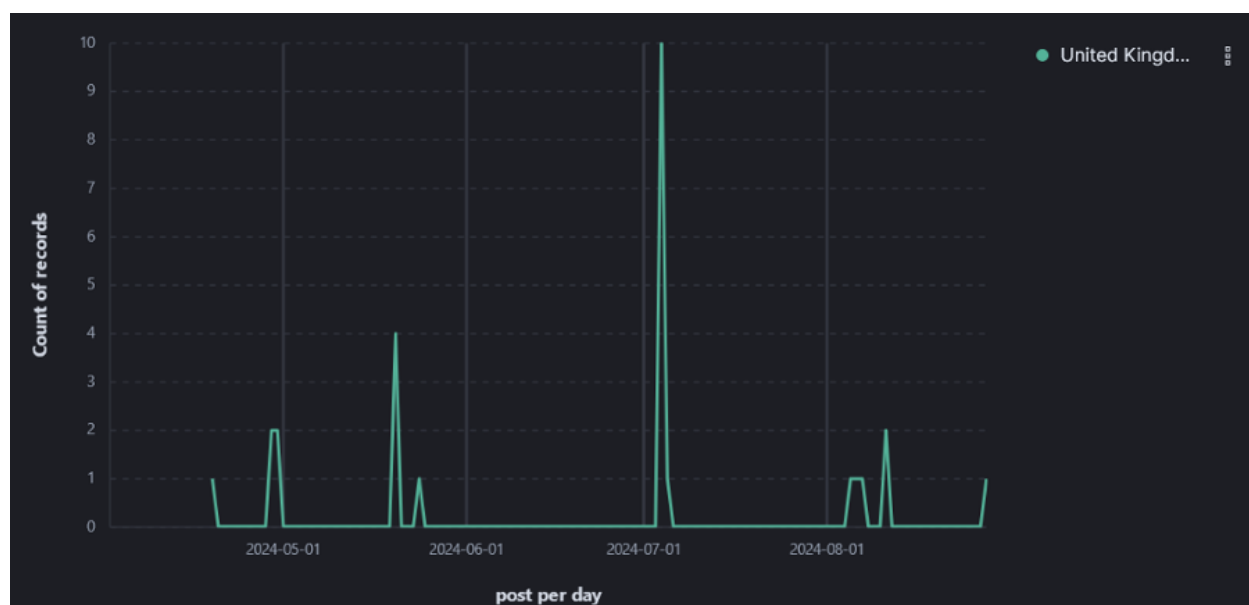


Figure 2: Graph to show CheckHost reports for attack claims against the UK in the last six months

Over the past five months, Cyjax has observed four principal spikes in hacktivist groups claiming DDoS attacks against UK-based organisations. These spikes occurred in mid-April, late April, early July, and early August. These attacks were conducted by multiple Russian-speaking groups, including [@NarodnayaCyberArmiya](#) (The People's Cyber Army),

@NoName057(16), @RipperSec, and @CyberVolk. Figure 2 shows the volume of attack claims against UK-based organisations according to CheckHost reporting per day. There are very noticeable peaks in activity, followed by lulls in attack claims. The attack claims occurred on the following dates with the following quantities:

- 2024-04-19: 1 attack claim
- 2024-04-29: 2 attack claims
- 2024-04-30: 2 attack claims
- 2024-05-20: 4 attack claims
- 2024-05-24: 1 attack claim
- 2024-07-04: 10 attack claims
- 2024-07-05: 1 attack claim
- 2024-08-05: 1 attack claim
- 2024-08-06: 1 attack claim
- 2024-08-07: 1 attack claim
- 2024-08-11: 2 attack claims

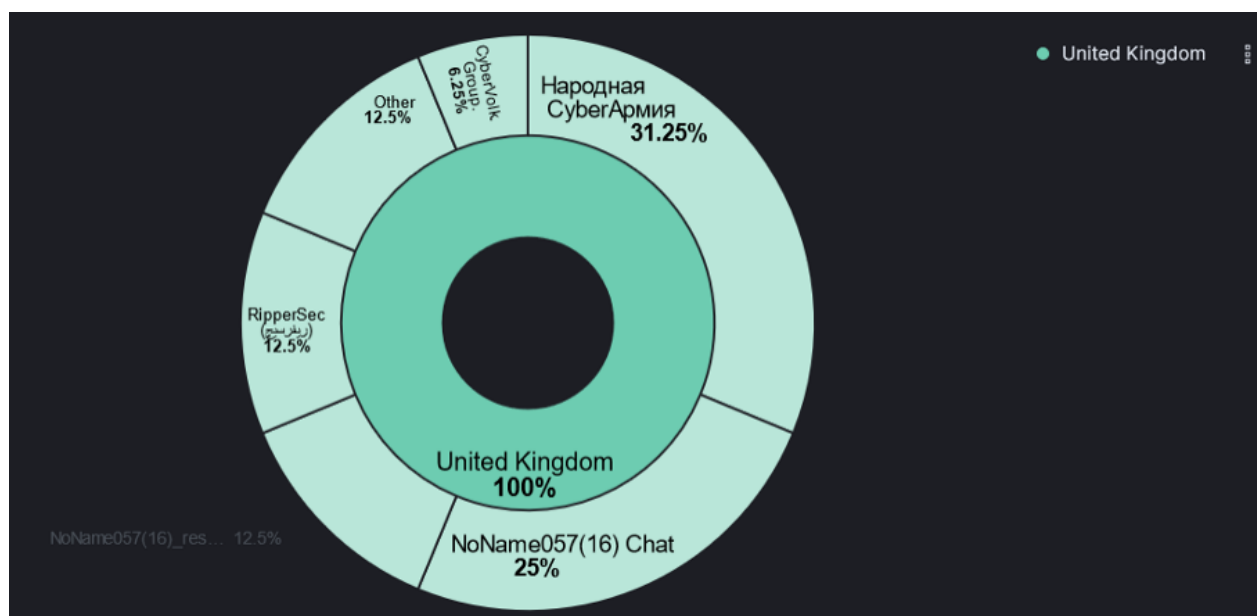


Figure 3: A graph to show the percentage of attacks claims against the UK per Telegram group

As shown in Figure 3, @NoName057(16) is the most active group according to CheckHost reporting of claimed attack against the UK, with it's two Telegram channels making up 37.5% of total attack claims.

Figure 4 further breaks down attack claims per day and separates them by group. This information can further assist in identifying which groups respond quickest to geopolitical event reporting and see whether there are any observable trends, such as if hacktivists follow another larger group with attacks.

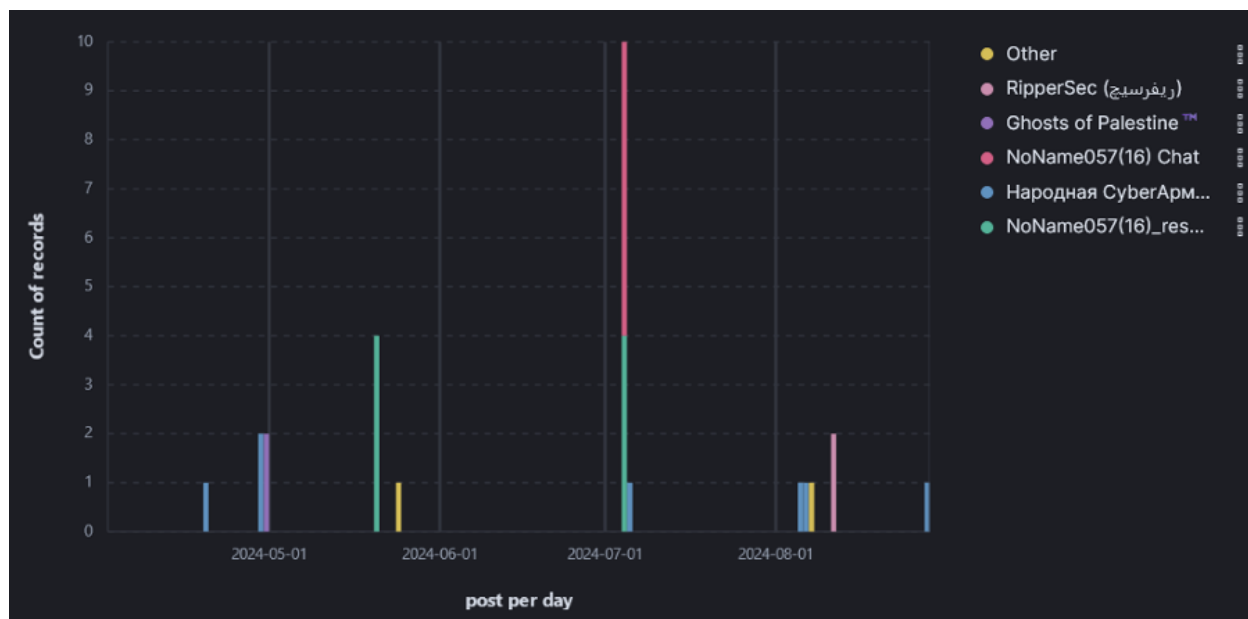


Figure 4: A graph showing a breakdown of attack claims per day, segregated by Telegram group

The four spikes

January 2024 security agreement

On 12 January 2024, former British prime minister Rishi Sunak visited Kyiv to meet with President Zelensky to discuss a support package for Ukraine. This resulted in an agreement being signed where the UK pledged a £2.5 billion support package, with additional sector specific support agreements being open to discussion in the future. This development in the Russia-Ukraine war was picked up on by hacktivist group @NoName057(16), who targeted several UK websites with DDoS attacks. Six attack claims were made in a post dated 15 January 2024, three days after major news publications reported on the agreement. Notably, the group stated that its attack was in direct response to Britain sending “*20 thousand military personnel to NATO exercises to fight Russia*”. Whilst @NoName057(16) had several public alliances with other hacktivist groups at the time, including with @22C, @CyberDragon, @NarodnayaCyberArmiya, and @FederalLegion, Cyjax could not find any evidence of these allies supporting the hacktivist’s efforts in this attack.

British Prime Minister Rishi Sunak and Ukrainian President Volodymyr Zelenskyy have signed an agreement on security cooperation. The signing of the document took place in Kiev, the Ukrainian head shared the relevant footage in his Telegram channel. Also Britain will send 20 thousand military personnel to NATO exercises to fight Russia.

Well while Britain is sending soldiers to the exercises, we are sending our DDoS missiles 🦹 to this country:

✗ **Confederation of British Industry**
(closed on geo) check-host.net/check-report/14a819fbk391

✗ **Swift card authorization** check-host.net/check-report/14a81bbfkd07

✗ **Authorization UK Finance - Merchant Organization** check-host.net/check-report/14a81d20kfec

✗ **Money Advice Service financial planning tips and guides** check-host.net/check-report/14a81e55k1c

✗ **Leicestershire County Council** check-host.net/check-report/14a82247kf88

✗ **East Cambridgeshire District Council**
(closed due to geo) check-host.net/check-report/14a82390ka11

Figure 5: A screenshot of the post made to NoName057(16)'s English mirror Telegram channel

May 2024 British-Finnish partnership agreement

On 20 May 2024, major news publications reported that the UK and Finland would be signing an agreement to pledge joint support for Ukraine against Russia. With this, the foreign ministers of Finland and the UK argued in a statement that “*Russia’s illegal invasion of Ukraine has fundamentally changed the European security environment*”, and vowed to support Ukraine’s recovery, reconstruction and modernisation in the aftermath of the conflict. This news was quickly picked up on by @NoName057(16), which claimed several new

DDoS attacks against government and critical national infrastructure (CNI) organisations in both the UK and Finland in retaliation on 21 May 2024. In the post, the group states that it was “test[ing] the strength of the internet infrastructure of these two Russophobic countries”.

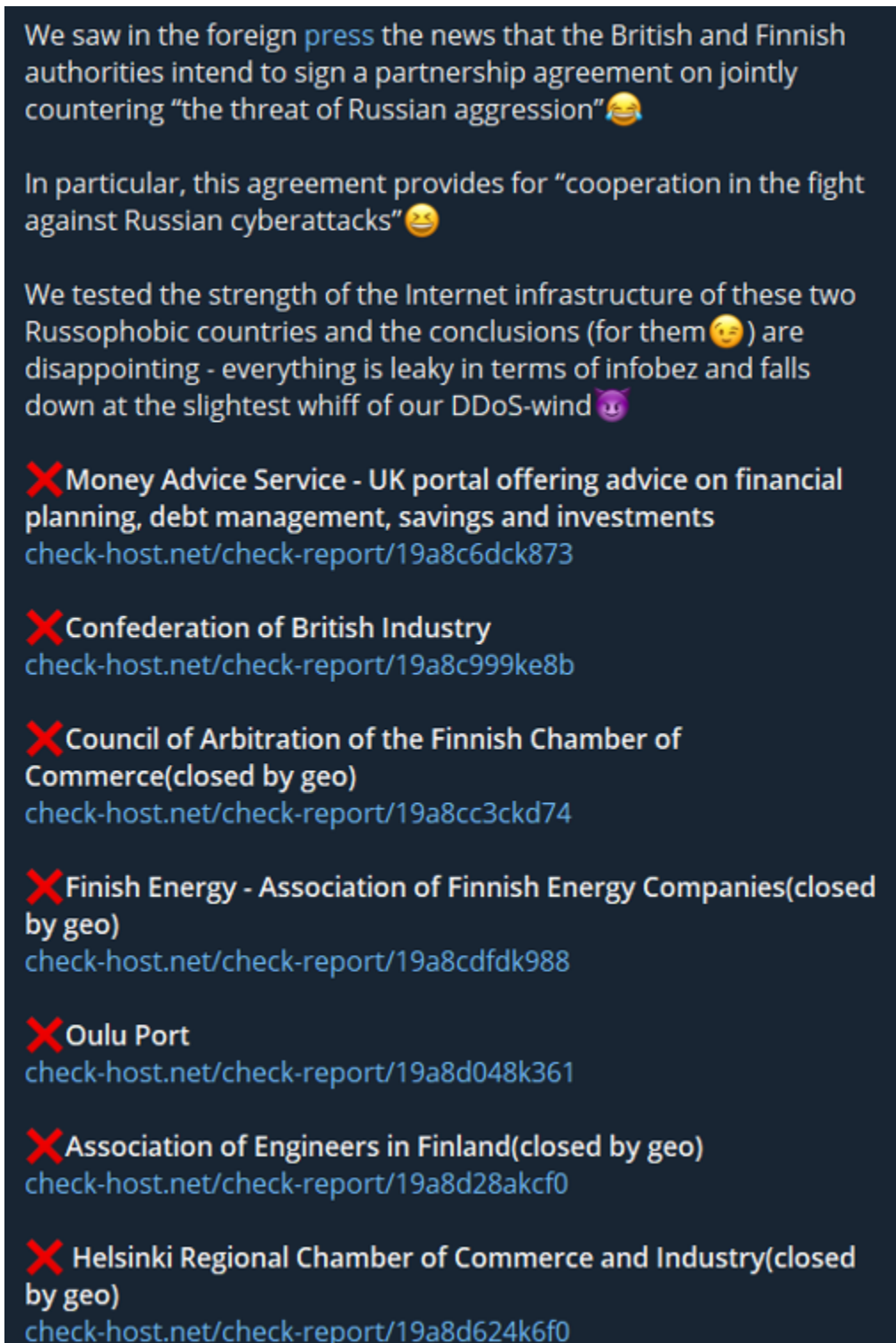


Figure 6: A screenshot of the post made to NoName057(16)'s English mirror Telegram channel

These attacks coincide with the data displayed in *Figure 2* and *Figure 3*, showing a surge in targeting of the United Kingdom. However, this also has an overlap in targets previously claimed in the January attack, when pro-Russian groups also claimed DDoS attacks against the Money Advice Service and the Confederation of British Industry. The CheckHost reports are different and imply that the group conducted a new attack against the same targets.

This reveals some interesting potentials surrounding the group's activity. @NoName057(16) is likely keeping a log of previously targeted websites which were successfully affected by its DDoS attacks. The list of victims can then later be reused by the group in future campaigns, if the targets has not upgraded its DDoS protection capabilities in that time. However, this is speculative and there is no verifiable way to confirm this.

July 2024 UK general elections

The 2024 UK General Election was held on 4 July 2024. The election saw 650 members of Parliament elected to the House of Commons. The opposition Labour Party, led by Keir Starmer, defeated the governing Conservative Party, led by Rishi Sunak, in a landslide victory. This was an incredibly significant event in the UK, one which has impacted domestic and international operations. Several Russian hacktivist groups quickly picked up on public reporting of the event, including the exit polls.

Pro-Russian groups likely took interest in this political event as it has the potential to significantly impact the UK's response to the Russia-Ukraine crisis, and could lead to further support to Ukraine and even a potential increase in frequency. @NoName057(16) notably responded on the day of the elections by targeting several public sectors, including transportation, city councils, and advice services. An attack campaign was started, which @NoName057(16) sparked with a call to arms against a country it labelled "*a stronghold of russophobia*".

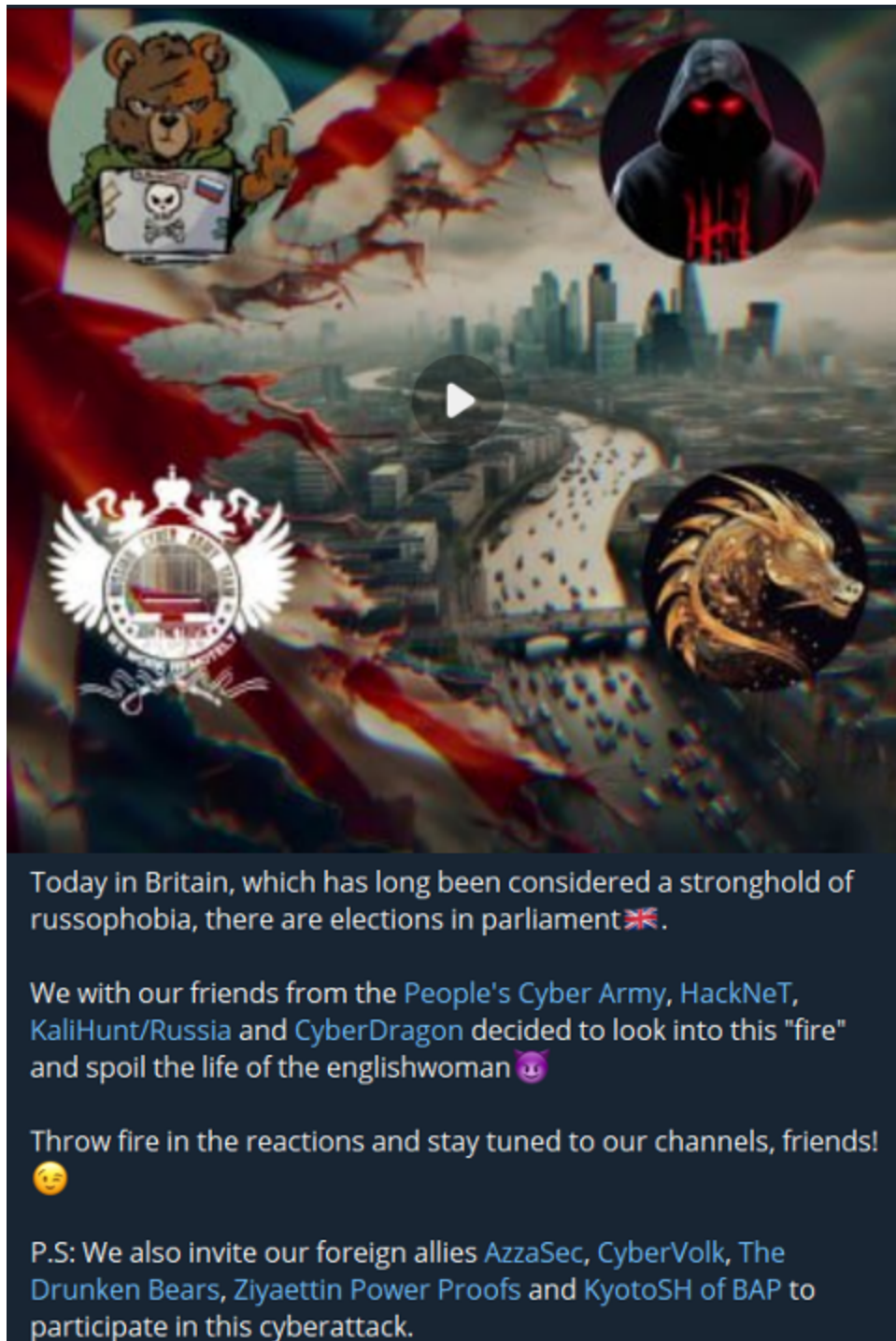


Figure 7: A screenshot of the post made to NoName057(16)'s English mirror Telegram channel

Figure 7. shows that out of the groups that @NoName057(16) called to action, only the People's Cyber Army, also known as @NarodnayaCyberArmiya, responded with an attack on 5 July. This occurred one day after @NoName057(16)'s initial attack wave against a UK government website. However, further investigation revealed that @HackNet also targeted the Scottish National Party (SNP) website on 4 July 2024. The significant spike in attacks

here shows that pro-Russian groups are not only keeping track of significant political events in the UK but are also able to respond in a significantly short time period with attacks. In this case, attacks began on the same day.

RipperSec's August 2024 attacks

RipperSec is a pro-Palestinian hacktivist group which conduct attacks against countries it perceives to be pro-Israel or acting against the interests of the Palestinian people. There was a slight spike in August in attacks targeting the UK, specifically the BMCE Bank main website. The claims were made on 11 August 2024 to RipperSec's main Telegram channel.

United Kingdom: BMCE Bank Website Down By RipperSec ⚡ 🇬🇧

-> Our Message 📄 :

🇮🇸 Open Your Eyes !! This is Genocide not Self Defense 🇮🇸

#FreePalestine #ForJustice

-> POC // Report 📄 :

<https://check-host.net/check-report/1d07e4c7k4f3> ❌

Location	Result	Time	Code	IP address
Brazil, Sao Paulo	Connection timed out	184.21.56.120		
Bulgaria, Sofia	Connection timed out	184.21.56.120		
Canada, Saint	Connection timed out	184.21.56.120		
Canada, Vancouver	Connection timed out	184.21.56.120		
France, Paris	Connection timed out	184.21.56.120		
Germany, Frankfurt	Connection timed out	184.21.56.120		
Hong Kong, Hong Kong	Connection timed out	184.21.56.120		
India, Hyderabad	Connection timed out	184.21.56.120		
India, Mumbai	Connection timed out	184.21.56.120		
Indonesia, Jakarta	Connection timed out	184.21.56.120		
Iran, Tehran	Connection timed out	184.21.56.120		
Italy, Rome	Connection timed out	184.21.56.120		
Japan, Tokyo	Connection timed out	184.21.56.120		
South Korea, Seoul	Connection timed out	184.21.56.120		
Spain, Madrid	Connection timed out	184.21.56.120		
Sweden, Stockholm	Connection timed out	184.21.56.120		
Switzerland, Zurich	Connection timed out	184.21.56.120		
Taiwan, Taipei	Connection timed out	184.21.56.120		
Thailand, Bangkok	Connection timed out	184.21.56.120		
UK, London	Connection timed out	184.21.56.120		
USA, New York	Connection timed out	184.21.56.120		
Vietnam, Hanoi	Connection timed out	184.21.56.120		
Yemen, Sana'a	Connection timed out	184.21.56.120		

Is Bacesmces.com down?

It's not just you! bacesmces.com is down.

Last updated: Aug 11, 2024, 1:07 PM (1 second ago)

Figure 8: A screenshot of the post made to RipperSec's Telegram channel

The attacks were made in support of Palestine, with the group labelling Israel's actions as "*Genocide not Self Defense*". However, it did not specify why it was targeting the UK, though the country was experiencing riots at the time. Typical of hacktivist activity, groups will often opportunistically attack targets within countries that it perceives as acting against its own core beliefs. Therefore, there could be spikes in activity like this one which are unrelated to an active event and rather a more general attack targeting a country rotationally.

Sectoral trends

From the attacks described above, the following sectors have appeared in attack claims:

- Energy
- Transportation
- NGO
- Financial
- NGO
- Infrastructure

These sectors are targeted specifically to cause disruption to services, which is likely to impact both the entity and civilian users. If an attack is successfully conducted, it will get picked up on not only by the targeted organisation, but the general public that use these services too. Third-party news reporting can often follow these attacks. Hacktivist groups rely on publicity in order to add to their image and spread their message, which third-party news reporting can help bolster.

The most notable trends observed in this monitoring period is the re-targeting of previous attack victims. Both the Money Advice Service and the Confederation of British Industry previously claimed to be targeted by @NoName057(16) in two separate efforts that were months apart, namely in January 2024 and May 2024, respectively. This suggests that these groups are logging successful DDoS attack targets for the potential to attack again in future campaigns. The Money Advice Service is a particularly large target that has the potential to cause disruption to a lot of people within the UK, especially during the rising cost of living. This target appears to be chosen deliberately, rather than the opportunistic trend which Cyjax has observed from several other hacktivist groups.

Concluding remarks

From analysis of the attack claims made against the United Kingdom over the last six months, clear patterns have appeared. @NoName057(16) leads the hacktivist space in terms of frequency of attacks and organisational competence. The group has shown that it can react in an increasingly short timeframe. Starting from the January attacks shown in *Figure 1*, the hacktivist responded in a matter of days. By the time of the July 2024 attacks, the group was responding on the same day with attack claims. @NoName057(16)

has also displayed the potential ability to influence other groups, as seen with the attacks orchestrated against the UK in July, in which numerous groups were involved. The People's Cyber Army were quick to also attack the UK at this time, acting a day after @NoName057(16). In terms of sectoral targeting, the groups appear to focus on public sectors, including transportation, energy, government, and infrastructure. This has the potential to cause significant disruption to both the targeted entity and civilians.

There are several predictions that can be made based on this data about future attacks. As shown, it is likely that pro-Russian hacktivist groups will respond within hours to three days at most. High level public facing services are shown to be at significant risk around the time of third-party reporting of geopolitical events. Therefore, entities within these targeted sectors, and more specifically previously targeted organisations, should be on higher alert and ensure that adequate DDoS protections are in place to mitigate potential disruptions.