Summary

This report summarizes a series of 3 separate digital and physical security threats and attacks directed at 4 prominent leaders of the BDS and Palestine Solidarity Working Group at the 2023 DSA Convention and in the days immediately following it. As the report lays out, these recent incidents continue a trend of threats against the BDS WG, its membership, and especially its prominent leaders.

Incident #1

On Sunday, August 6th one of the BDS WG's leaders (Leader #1) gave a floor speech during debate over NPC Recommendation #8 which concerned the heightened risk of doxxing faced by Palestinian and Arab organizers in DSA so long as DSA allows Zionists to remain members. Immediately following the speech, there was an attempted hijacking of the leaders' phone while it was connected to the DSA Convention WiFi (SSID: dsacon2023). This consisted of an attempted unauthorized transfer of the Signal account to an unknown device (see here for transfer method). The leader experienced this attempted data hijacking 3 times before leaving the Convention hall and disconnecting from the WiFi. Less than 30 minutes after these first hijacking attempts, another leader of the BDS WG (Leader #2) faced the exact same attempted hijacking via unauthorized Signal transfer, also while on the Convention WiFi. The second leader immediately disconnected their phone from the WiFi and did not experience additional attacks. Additionally, another leader of the BDS WG (Leader #3) likely also had their Signal account targeted after receiving consecutive pin and CAPTCHA verification requests within the same narrow time frame. While the source of these notifications is unclear, the difference in behavior could be attributed to the attacker not having a compatible device (Android device) or the device not having either Bluetooth or WiFi on.

This incident demonstrates that not only was the digital security of BDS WG leaders compromised at DSA Convention, but also their physical security, as this type of Signal transfer can only be initiated within physical proximity (determined via Bluetooth, which requires a distance of less than 33 feet) while on the same WiFi network as demonstrated by the requirements for this transfer method on the Signal website. It also requires knowledge of the actual identities of the leaders and the personal phone numbers of said targets (Signal assumes phone numbers as unique identifiers). This very likely demonstrates a politically motivated attack, given the nature of the attack starting immediately after the first leaders' floor speech concerning the threats of doxxing for Palestine organizers. This attack had to be executed by someone in the DSA convention hall – therefore, either someone DSA had granted access (delegate, staff, observer, press, etc.) to enter the space or a fraudulent infiltration.

Incident #2

On Saturday, August 12th, another leader of the BDS WG (Leader #4), who had also given a floor speech during debate over NPC Rec 8, experienced a crash of their Whatsapp desktop application. Immediately after the crash, the leader opened a page on Facebook and the entire Facebook interface (menu options, descriptions, etc.) appeared in Hebrew. The leader was not

running a VPN that could have caused the website to sense a connection from another country and change the language accordingly; nor did the leader access the page in Hebrew from a third party website (e.g. Google), but rather the interface language changed then they opened a new page while already on Facebook. The page they were visiting did not appear to have any connection to Israel, and after refreshing the page, the interface appeared normally in English again. The leader immediately restarted their laptop, but after restarting it, the same issue happened a second time in the same fashion. Separately, a different BDS WG leader (also a target in Incident #1) received multiple recovery attempt emails for their private Instagram account the day following the convention. The WhatsApp, Instagram, and Facebook platforms are all owned by Meta.

Incident #3

On Tuesday, August 8th, one of the BDS WG's leaders (targeted under Incident #1) who played a prominent role in the BDS WG's organizing at Convention had returned to their hometown and was accosted by a stranger who delivered a letter that referenced their Palestine organizing work (their primary work in DSA). More specifically, the leader was in an establishment they don't regularly frequent. The letter strongly discouraged them from further Palestine organizing and concluded with a thinly veiled threat. This incident demonstrates a serious threat to the physical security of this leader. The fact that this happened to one of the leaders whose phone was also subject to the attempted Signal hijacking in incident #1 establishes a pattern of targeting against this leader and begs the question of what data was compromised at DSA convention.

Follow-up

Since the attempted digital breaches and physical threats, the devices were checked by third-party security researchers for signs of unauthorized access. The checks came up clean. Further follow-up is underway with regards to possible unauthorized access of social media accounts. The individuals mentioned have since pursued more thorough security measures to protect themselves and their loved ones. No further incidents have yet been reported. While the identity of the malicious actor(s) remains unknown, we've escalated the incident with relevant parties to track it down.

Conclusion

The coordination and knowledge required for this pattern of targeting suggest a more determined adversary with access to internal DSA communication channels and information as well as access to the DSA convention hall/WiFi. Prior to convention, the BDS WG had blocked attempted infiltration of its internal communications channels by a number of potential malicious actors and reported it to the NPC. The BDS WG's social media accounts had also been subject to heavy brigading and targeting by right wing and zionist elements ranging from elected officials to Zionist coalitions directly litigating the content of the accounts. While there's a pattern of malicious actors targeting the working group, these latest incidents represent a further escalation from digital space into physical space.