FILED UNDER SEAL

EXHIBIT 13

Subject: [Interop External Engagement XFN] Status Update

From: [redacted] <[redacted]@fbworkmail.com>

Date: Sat, 26 Oct 2019 12:45:24 -0700

To: Interop External Engagement XFN [redacted]@mail.workplace.com>

Bcc: Nick Clegg <[redacted]@fb.mail.onmicrosoft.com>

[redacted] posted in Interop External Engagement XFN

26 October at 12:44

[redacted]

25 October at 03:27

Remediation: Detecting Malicious Networks (CEI), Integrity E2EE Taskforce - Investigation Insights

TL;DR

As part of the wider work on the Integrity E2EE Taskforces: Remediation: Malicious Networks (CEI), investigators from Online Safety and CO Safety Investigations conducted deep-dive analyses of three separate CEI traders and their immediate network in order to gain qualitative insights into their behaviour on Facebook.

Key findings include:

Group message threads often had many participants (100+) with virtually no commonalities in geographic location, groups, pages, friends, etc.

Search history sometimes revealed very explicit search terms, names of accounts, or known bad websites.

CEI traders often used multiple fake accounts and represented themselves as male or female minors depending on their sexual preference.

CEI traders focused mostly on CEI, but there was also overlap with adult pornography, particularly involving paraphilia (i.e. extreme sexual deviance) and other fetishes.

A number of product and policy recommendations resulted from these investigations and are outlined in the note.

One big question which remains only partially answered relates to exactly how CEI traders are able to find each other on Facebook, and this will be an area for additional analysis.

Purpose of note

This note provides an overview of findings from three deep-dive investigations conducted by investigators from Online Safety and CO Investigations teams as part of the wider work of the CEI taskforce. The investigations were designed to provide a qualitative analysis of known CEI-trading networks on Facebook and to give insights into the content of such threads and the behaviours of the accounts involved which could help inform the development of post-end-to-end encryption detection and prevention of CEI distribution. The findings are based on specific networks of CEI traders rather than large-scale analysis of accounts disabled for CEI distribution. It is important to note that the focus of investigations was on Facebook users trading large amounts CEI with egregious or malicious intent - we did not look at other child safety abuse areas such as IIC or sextortion, and we did not look at user activity on Instagram or WhatsApp. The note outlines the main findings and recommendations, but also includes more detailed findings from each individual case study for deeper understanding.

Taskforce Overview

The end goal of the E2EE CEI Taskforce is to ship privacy preserving behavioural and account level detection for malicious CEI network building. We did this by understanding CEI trading behaviour on Facebook and identifying signals that are not dependent on content and which can be used post-E2EE to detect trading of egregious CEI on Messenger. Historically, CEI trading has been seen as a content rather than a behavioural problem, meaning that efforts were prioritised for detecting and reporting CEI versus looking more deeply into the behaviours of those accounts engaging in CEI trading. With the impending arrival of E2EE and with over 85% of reported CEI coming from Messenger, it became necessary to work towards understanding the behaviour of such accounts in order to detect them in future, without relying on confirmation via reported content.

In order to better understand the problem, CEI trading behaviour was broken down into different types:

Egregious intent (most severe content shared for the purposes of sexual gratification - e.g. minors being sexually abused - 20% of recent media shared is A1-B2 (i.e. most explicit/egregious) CEI or the thread contains off-platform links to CEI collections),

Sexualising intent (less severe content shared for the purposes of sexual gratification but which in other circumstances could be considered innocent, e.g. an under-clothed child at the beach),

Innocent/borderline intent (less severe content shared in an unclear context) and other (content of varying severity shared in non-sexual context, e.g. outrage, raising awareness, attempted humour etc.).

The taskforce initially explored egregious intent CEI sharing in both group and 1:1 threads. In order to maximise the generalisability of our learnings, we decided to prioritise our resources on detection/measurement of egregious group threads. We believed this was more generalisable to other problems like terrorism. There are items on the Child Safety roadmap to better understand actor level/1:1 threads in Q4. Additionally, accounts in egregious intent 1:1 threads are often also in egregious intent group threads (46 out of 69 examples, 67%), so we felt comfortable shifting to focus on group threads only for the purpose of the taskforce. however

The taskforce comprised of individuals from Online Safety, Community Operations and I2, and the role of the investigators within this taskforce was to conduct deep-dive investigations into egregious CEI traders and seek to answer questions relating to 1) the dynamics of group message threads engaging in CEI trading on Facebook; 2) the relationships between the participants in these threads, and 3) the behaviour of the most active participants in these threads.

Investigation Process

Over 400 inboxes were reviewed by investigators in the course of working on the taskforce, and these were identified in a variety of ways: [redacted] Each investigator chose a CEI trader of interest as a starting point from which to fan out and identify a wider CEI trading network, resulting in three unrelated deep-dive investigations into different networks. All three investigators chose unrelated cases and there is no direct connection between any of the individuals.

Key Findings

Account Level Findings

CEI traders tended to use fake accounts (0.4 FAI average, often lower) and often represented themselves as either male or female minors. They tended to represent themselves as the gender they were interested in - for example, CEI traders focussing on female minors would present themselves as female minors.

CEI traders also tended to have multiple fake accounts (61/205 with FB SUMA accounts), with one responsible having up to a dozen fake accounts appearing on the same DATR. Many of these accounts had already been identified and disabled by our systems by the time the investigators found them, thus explaining the need to create additional accounts. The disable reasons were not always CEI-related however, with many being disabled for being fake accounts.

CEI traders tended to focus more on CEI than other types of sexual imagery, however overlap did exist with adult pornography particularly involving paraphilia such as bestiality, bondage and other fetish imagery.

Search history sometimes revealed very explicit search terms indicative of interest in CEI, either as explicit terms, names or known websites (e.g. “kids porn videos”). However, search terms more often related to specific names of accounts and would not be indicative of CEI trading on their own.

[redacted]

Overall, CEI trader account behaviour did not tend to overlap with other abuse types such as sextortion, grooming etc. and followed their own pattern of behaviour and characteristics.

Group Thread Level Findings

Group message threads almost always contained either links to WhatsApp groups or shared phone numbers with the explicit intention of sharing CEI via WhatsApp. This echoes the findings of a recent note showing that a large number of CEI trading on WhatsApp originates from links shared on Messenger threads.

Group message threads dedicated to CEI trading frequently had explicit titles or at least strongly suggestive of CEI or minor sexualisation content (e.g. “‘Dark Room’ childporno”, “SWEET KIDS♡♡♡”). They also tended to focus on CEI of either male or female minors, rarely both.

Group message threads tended to be large (100+ participants), with participants constantly being added or removed from the thread.

Group message thread participants tended to have virtually no commonalities in terms of geographic location, common groups/pages, friends in common et cetera (ex: one thread with 138 participants included accounts from over 30 countries with a maximum of 9 accounts member of a same group, 7 accounts liking the same page, and 28 friends in common among participants).

General Platform/Tool Findings

There is no threshold on how much CEI one can receive. We found users included on hundreds on NCMEC reports as recipients with no enforcement or account review.

PYMK appeared to be an important way that CEI traders found each other, and common friends seem to be the way a lot of accounts came into contact with each other. However the question as to how newcomer CEI traders find each other is still open, with off-platform sources a potential partial answer as well as reaching out to other individuals in groups or pages which could be of

interest to CEI traders (eg. groups or pages where minors are likely to be present, which relate to sexual paraphilia or which sexualise minors in some way).

Signals and techniques most effective in understanding the threat + and how can they be leveraged for future discovery of this abuse type

a) Account representation

CEI trading accounts represent as a mix of genders, highly dependant on the gender of CEI they were trading - i.e. purporting to be females if they were trading female CEI.

The spectrum of the ages the accounts claim to be ranges from 13 to 65, however the median age skews younger, reflecting the fact that CEI traders often represent themselves as minors on the platform. A consistent theme amongst the profiles was the use of minors as their profile images.

Most accounts were disabled relatively shortly after creation (<100 days) however a large minority were not, with one notable account being active for 1454 days before being disabled. There were several signals that would indicate this account was involved in activity inconsistent with community standards. His cover photo was a picture of women's underwear and he had been blocked from 10 groups and was a current member of 752 groups. The groups he had been blocked by were fetish-themed such as 'Humiliated by a group of women', 'Wife and Girlfriend showoff', 'Sissy Planet' and 'Candy Shop'. The themes of the groups he was a member of include 'Hot girls', Cross-dressing/'sissy'/Transgender, 'Teen trans/traps/cd/sissys', Fetish – bondage, role playing and 'Teen dating Groups'.

Accounts also tended to accumulate large numbers of friends despite being disabled relatively quickly, for example accounts could have 50+ confirmed friends after being active only a couple of days.

CEI trader account location spanned the globe, with Antarctica being the only unrepresented continent in these investigations. Certain countries appeared slightly more frequently - Brazil, Philippines, Iraq, Pakistan - but on the whole CEI traders appeared to be very international.

b) Group Membership

Although we did find incidental CEI group membership, it was not consistently high across the subjects of investigation, with approximately 10 groups per account on average. However, the theme of the group tended to be sexualised (wife swapping, polyandry etc), fetish related or targeted at teens or sexual preference support groups such as Transgender or lesbian. There was also an instance of a CEI trader being a member of a rape/incest support group.

Members of the aforementioned "CEI groups" were not posting CEI per se, but the intent was pretty clear from the names and posts, either asking for CEI or publicly sexualising minors via comments and images. Examples of group names include [redacted]

c) Group Administration

Group administration was not prevalent in this cohort with only one individual being the administration for a 'hot girls' group that posted sexualised images of young women, however the group only had two members of which he was one.

d) Page following/administration

Intent of CEI trading is less obvious on pages than groups. Behaviour on pages is more about minor sexualisation (as a potential signal of CEI trading intent in more private spaces such as Messenger or secret groups). Examples of topics of pages followed include kid modelling, teen dating, etc.

There was only one instance of a Page being administered by a CEI trader and this page was disabled for minor sexualisation. The page was called [redacted]' and was intended to generate sexualised images.

e) Search terms

Many accounts identified in these investigations did not have explicit CEI or sexualised search terms in their search history. However, those that did included very explicit terms consistent with sexualised interests, and more specifically child related searches.

[redacted]

[redacted]

Another trend was for CEI trader accounts to search for specific names, either of real minors or of other CEI trader accounts. It is likely in these instances that the names were known to the CEI trader either from off-platform discussions or from on-platform interactions via previously-disabled accounts, however this area needs additional research.

f) DATRS and convergence of abuse accounts on same DATR

The vast majority of identified CEI trader accounts had DATRs containing previously disabled accounts, with disable codes including:

[redacted]

g) Friending behaviour

CEI trader accounts tended to have relatively high friend rejection rate (25%+), and tended to send friend requests to accounts representing the gender they are interested in (e.g. if CEI trader interested in female minors, tends to send 75%+ of friend requests to accounts representing females).

h) Media Matching

We created a NCMEC-reportable bank for previously-unknown CEI uncovered during our investigations. We banked 116 images and 246 videos over the span of two months, resulting in 32.3k pieces of media reported to NCMEC and 25.7k users removed from the platform. We also used the MMS bank hits as seed content to review uploaders and threads.

i) Groups threads

Accounts tended to participate in group chat threads dedicated to sharing CEI, adult pornography, sexualised minors or a combination. Most group chat names were explicitly referred to being for child imagery – [redacted] etc.

Group threads could contain up to hundreds of accounts, with participants located internationally with no obvious commonalities. Accounts tended to be added to the group thread throughout its lifespan, with accounts also leaving throughout. Links to WhatsApp group threads were shared, as were links to file sharing websites. Live video chats occurred in several examples, however there was no indication as to what these contained.

Product and Policy Recommendations

Automatically enqueue users for review if they are associated with a certain number of NCMEC reports - our investigations have shown that some users may be attached to over 300 NCMEC reports as recipients yet still be active on the platform. This is a gap where regular recipients of CEI are being overlooked by the system. T56293914

[redacted]. T56343242

[redacted]. T56293914

Although further research is needed to confirm exactly how CEI traders locate one another on the platform, the fact that CEI traders tend to create new accounts and appear to search for accounts they know suggests that a possible prevention tool could be to enqueue for review users searching for accounts which have been disabled for CEI or related abuse, or which are SUMA accounts of users disabled in this way. T56293914

Accounts searching for CEI-related terms or for names of sites known to host CEI content should be enqueued for review. T56293914

The evidence of some CEI traders also trading non-CEI sexualised images of minors or being active in groups or pages suggestive of minor sexualisation suggests this could be another area which we need to understand more deeply.

Newly created accounts sending a large number of friendship requests to accounts with high FAI score or otherwise suspicious accounts could be enqueued for review. T56293914

[redacted]. T56343326

Users should be given the option to accept or decline being added to a group thread, as this would remove the possibility of innocent accounts being implicated with CEI-trading threads, and allow them to avoid this negative experience themselves. T56343360

Overall, individuals engaging in egregious CEI trading tended to use fake profiles for carrying out this activity, often impersonating minors. Age verification and Fake Account checkpoint enrolment for suspected CEI traders could be an effective way of preventing them from operating on the platform in the absence of definitive proof of CEI trading from Messenger content. T56293914

Action Items/Next Steps

The findings of these investigations have been shared with the rest of the taskforce and inform the efforts at building a classifier for encryption-proof proactive detection of CEI traders in group message threads. However, the question of how CEI traders find each other is still one which needs closer attention, and so future work will be done in this space in Q4 (Leah, Luca, Hedda, Melanie).

Additionally, a closer analysis of possible links between Facebook, WhatsApp and Instagram CEI-trading behaviour should be made in order to gain a more holistic understanding of CEI trading behaviour in the family of apps.

Thanks to Melanie [redacted] (Threat Investigator/OS-I3) and Johanna [redacted] (Safety Investigator/CO Safety) for conducting the investigations and identifying key insights, to Luca [redacted] (Data Scientist/OS-I3) for providing data science support, Leah [redacted] (Programs & Partnerships/OS-I3) for ongoing input and feedback and Mike Gillin (Project Manager/CO Safety) for insights and data from CO Safety.

Appendix - Case Studies

Methodology

The methodology used was typically the following:

From the original suspect account, identify all linked accounts engaging in CEI trading with other accounts. Deeply understand this individual's behaviour via his multiple accounts and understand how he identified/contacted other CEI trading accounts.

From the CEI trading accounts identified in 1), identify:

Additional accounts belonging to the same responsibles,

Group threads dedicated to sharing CEI in which they are a participant.

From the CEI sharing group threads identified in 2), identify:

The most active traders,

How the thread participants relate to one another,

How the group threads relate to each other (degree of overlap).

Investigate the most active traders in these groups and identify:

Additional accounts belonging to same responsibles,

[redacted]

Case Study 1

The subject of this investigation was originally misidentified as
a case of minor content sextortion (i.e. someone who coerces minors to produce CEI using blackmail). This was part of a proactive effort to identify content sextortion on accounts using TOR, which is of interest to us since this hides their true IP, makes it harder for us to identify linked accounts or identity of the responsible and, in Online Safety's experience, is often associated with more severe abusive behaviour. In this case the responsible appeared to be operating out of southern Italy, however upon closer inspection the abuse did not appear to consist of content sextortion. The case triggered Online Safety's interest however because, although without merit as a content sextortion case, the individual was also in communication with accounts apparently engaged in CEI trading. These accounts tended to share no common features with the original suspect's account or with each other, and it was unclear how they had identified each other on the platform. Investigation of these CEI trading accounts' inbox revealed the presence of large group threads dedicated to trading egregious CEI content (both images and videos) and links to a wider network of accounts trading CEI.

The original Italy-based bad actor had a total of five fake accounts used for the purposes of attempted IIC and CEI trading, though he did not engage in the most severe abuses in this space

(no evidence of having abused a minor offline, no successful content sextortion and only very limited CEI involved). An authentic account belonging to the responsible was not identifiable. The DATR was small, containing only a few additional accounts, all inauthentic, clearly belonging to the same individual. The fake accounts tended to use images of female minors as profile photos, claimed to be a minor and belonged to groups or pages likely to appeal to minors (schools, teen dating etc.), indicating probable grooming behaviour. All the identified accounts had already been disabled by the time the investigation started, however not before they had a chance to contact real minors and CEI traders. Search terms tended to refer to either names of specific individual accounts or to groups/pages. No explicit CEI terms were used in search by any of the linked abusive accounts, and it appears the CEI trading accounts which were befriended and/or engaged in conversation were suggested by the PYMK feature - all had friends in common. They tended to have been blocked by a relatively large number of accounts belonging to minors (26 total), and this appears to be a trend in accounts attempting to engage in CEI trading. Conversations with CEI traders were initiated by the Italy-based user and the pretence was maintained that both participants were minors - it is unclear if the CEI trading accounts genuinely thought the responsible was a minor and were attempting grooming, or else if they suspected the true nature of the situation and chose to stay "in character" as a precaution. Regardless, the most interesting aspect of this individual's behaviour was his connection to more serious CEI trading accounts rather than any abuse he was engaged in directly.

These other CEI trader accounts were used by individuals located in Croatia, Brazil and the USA, and each had multiple linked fake accounts also engaging in CEI trading behaviour. The smallest cluster relating to a single person was 5 accounts belonging to an individual located in Brazil, and the largest number was 21 accounts belonging to an individual in the USA. None of these made extensive use of TOR or other proxies, and identification of the responsibles' authentic identities was relatively straightforward by fanning out via DATR, device and/or IP address. These accounts were involved in large group threads explicitly dedicated to sharing CEI material. Also, all these CEI traders used images of minors as profile pictures, many of them in suggestive but non-violating poses (e.g. young teenage girl in swimwear).

Between the four accounts which came into contact with the original Italy-based suspect, nine CEI trading group threads were identified, with little to no overlap between participants. Some had no name, but many had explicit titles making their purpose clear: [redacted] for example. The groups varied in size, with the largest containing 138 members and the s[redacted]est 17 - however the majority contained in the region of 100. Among these members, only a relatively small number of participants actually posted content, with a large majority seemingly happy to "lurk" but not participate directly. On average no more than half the participants actively engaged in the thread, though more often this proportion was smaller. Strikingly, the overwhelming majority of participants in these threads appeared to have virtually nothing in common: accounts would originate from dozens of different countries across the world (the only continent with no representatives was Antarctica!), multiple languages were used and there appeared to be no significant overlap in terms of common groups of pages. These threads were constantly evolving in terms of participants, with accounts either being added to the thread or leaving throughout its existence, however there was constant demand for CEI and frequent remonstrations against any member sharing non-CEI content (for example, adult

pornography). The CEI that was being traded in this investigation focussed on female minors being abused, and the use of female minors used as profile pictures perhaps is used to signal interest in female minors by the CEI traders. In several instances the thread initiator account had been permanently deleted and associated information lost; where the initiator was not deleted the country of origin varied (Philippines, Turkey and Brazil). This fits with the common theme of CEI traders being based all over the world and interacting with like-minded individuals on our platform regardless of geography or real world interactions with each other. Another trend in these threads was a lack of apparent commonalities between participants - out of hundreds of participants, only a handful of accounts might follow a common page, with larger numbers belonging to common groups however still a small minority relative to the wider population of thread participants. In terms of thread content, aside from CEI common features included solicitations for private messages, sharing phone numbers with the intention of making contact via WhatsApp, group video chat (no indication as to the content of video streaming), sharing URLs for file sharing websites (e.g. Megaupload) or sexualisation of minors (e.g. voting in child beauty pageant), as well as requests for especially sadistic content (e.g. video of infant being raped). There were indications that some people had been added unwillingly - one user appeared to be a real minor and asked to leave saying the thread was "rude" and expressed fear that her parents would find the content on her phone; another was posting religious content before being asked to leave. This suggests users can be added to threads without prior consultation or even being well known to the account adding them.

In terms of the most active participants in each thread, individuals which were actively involved in sharing CEI, work was done to understand more deeply how these individuals operated on the platform and how they interacted with CEI-sharing threads and with other users. The single most active user in each of these threads were extremely spread out geographically, being based in Australia, Iraq, Philippines, Brazil, Turkey and France. Only one of these most active CEI-trading accounts was authentic and the remainder used fake accounts. All actors had multiple Facebook accounts (up to 10), and each individual had had multiple accounts independently disabled prior to being identified as part of this investigation (sometimes for CEI violations, sometimes for being a fake account) but almost always had some abusive accounts still active. Four of the seven made extensive use of pictures of minors as profile pictures, with several using images of minors in potentially suggestive poses. All responsibles were adult men of varying age (20s to 60s). [redacted]

Only one of the most active users had an account representing his true identity - this was an older user (apparently in his 60s) located in France and who also engaged in grooming behaviour. He had multiple accounts which had been previously disabled and kept creating new ones both for authentic activity as well as abusive behaviour. Possibly because he was using his real identity, this responsible was the only user with linked Instagram accounts (incidentally also used for grooming attempts, but with much less activity than his Facebook accounts). Also of interest, although all the most active CEI thread participants were also involved in sharing adult pornography, this was relatively minimal and the focus tended to be more on either CEI or the sexualisation of minors. They also expressed interest within certain threads of less "mainstream"

pornography, such as pornography with transgender individuals or featuring scatophilia. However, no accounts identified in the course of this Case Study appeared to have access to minors for the purposes of exploitation or to be producing CEI content - all appeared to be consumers of CEI content rather than producers.

Case Study 2

Starting with one egregious CEI-sharing Messenger group thread reported by a user and escalated to Investigations via internal task, we fanned out into the most active users' inboxes and manually uncovered over 40 additional abusive threads, with membership count ranging from 10 to 250 users.

Some examples of names used for these group threads: [redacted]

We looked into how users had joined these threads by querying the messenger_thread_mutation table and found that 38.62% of members had been added by another user while 61.38% had joined using invitation links. While we were not able to pinpoint the origin location of these specific links, we found that users are commonly sending such invitation links in 1:1 threads as well as other CEI group threads. We also uncovered groups where users publicly express their interest in exchanging CEI media and links to such conversations, including links directing to Whatsapp groups threads (example of group with clearly violating name: [redacted]. Lastly, most of the 1:1 threads between users didn't have much text, mostly media, media requests and requests to be added to group threads.

Our next step was looking into which users were responsible for the creation of these Messenger group threads. We identified an account responsible for creating 6 out of the 40 group threads we looked into (referred to as Subject of Interest).

Deep dive into Subject of Interest:

Location: Indonesia

Registered Age: 14

Age Affinity: 14

Age of apparent authentic user: 19

Total Days on platform before disable: 22

Disable Reason: [redacted]

Number of friends: 1560 (of which 350, or 22.5%, were already disabled - this number increased to 770, or 49.4% by the time this investigation started)

Number of friends' accounts already disabled: 770 -- 242 (31.4%) of them for authenticity reasons and 528 (68.6%) for child safety violations.

Number of attached NCMEC reports: 307 (!)

Bio: [redacted] (unofficial translation: [redacted]

The account had been reported 32 times within its short lifetime (3 for Impersonating, 29 for FakeNotRealPerson as there is no option to report directly for child safety violations at the account level) and the content generated from the account had been reported 7 times (for Pornography). From one of these content-level reports, one post was escalated from a marketised Indonesian queue to a Child Exploitation review flow where the account got disabled.

It is interesting to note that the account had an astonishingly high number of NCMEC reports (307) associated to it - all as participant/recipient. [redacted]. While we understand concerns about automating actions on recipients of any content, we believe that accounts should be enqueued for review above a certain threshold.

The next step we took was to look at the 54 DATR-linked accounts (surprisingly enough there was no device-linked account). 42 were already disabled, mostly for authenticity reasons (failure to clear roadblocks). Almost all accounts were registered as 14 or 15 years old with high FAI scores. We dived into the 12 linked accounts that were still active: 5 were members of CEI trading group threads, with an average number of 68 NCMEC reports attached to their account (ranging from 26 to 187).

A common pattern of messaging behaviour we observed across all accounts investigated were a high percentage of message recipients being non-friends, registered as males. This could be caused by the group threads' activity and the CEI surfaced in this investigation being mostly boys - this audience was mostly interested in boys and thus were creating fake boys accounts as a way to communicate their preference (registered as under 18 and profile picture depicting a child).

This investigation also found that many friend requests are initiated after finding the profiles on People You May Know, hence the importance of building a behavioural, account-level classifier to avoid recommending such actors to each other.

Case Study 3

A notable case was that of an account based in Algeria first identified in a thread with another CEI trader representing as a female account based in Mexico. On 23 August the Algeria-based account posted on his profile status [redacted]" and on the 26 August the Mexico account initiated the first conversation.They became Facebook friends on the same day the conversation thread began with a "hello" and thumbs up and immediate exchange of CEI.[1] It is a current information gap how the Mexico account discovered the Algerian account.

These two offending accounts did not share membership or involvement with any common groups. Being from Algeria and Mexico they share neither a common language or geographic location yet still identified each other as having an interest in CEI. Both had a 25% rejected friend rate so it may be that the net is cast wide to large numbers of individuals in the hope that a small portion will have a mutual interest in CEI.

The two seed accounts did however have 10 mutual friends – from Colombia, Sri Lanka, Saudi Arabia, Venezuela, Mexico, Pakistan. No commonality or group membership convergence was identified but all mutual friend accounts represented as female accounts with minors depicted in the profile image. The Algeria-based account did initiate contact with the female accounts he shared with the other CEI trader to either attempt to groom because they were actual minor female accounts or because they were also accounts purporting to be minor females but were involved in CEI trading in separate 1:1 threads with other offending accounts.

The Algeria-based account presented as a 27-year-old male with a profile photo of a Caucasian male model. His account name was originally in Arabic script and was then anglicised to 'Ali Ali'. There were attempts by this account to compromise accounts of those he was in 1:1 threads with by sending a link which he claimed had a file with additional videos, but the UI to enter into the file asked for the user to enter their Facebook email and password. The Algeria-based account also asked users to join his WhatsApp group chats for CEI exchange and provided screenshots of the groups to show some of what was available.

There were 38 device linked accounts on the DATR for the Algeria-based account – of those 8 were disabled for explicit reasons such as CP or grooming. The remainder contained no offending content, belonged to family members of the attribution account and the attribution account himself. A review of the attribution account identified no offending content. With the exception of a fake accounts, there were no attempts made to obfuscate his identity.

From this 1:1 exchange between the two seed accounts, inbox review identified a CEI Group Chat with 33 participants. The Algeria-based account of interest, was the largest contributor of CEI to the thread. The bulk of the content in the thread was sexualised minors or B2 classified imagery. The Algerian account did not create the chat group in the first instance, however invited the bulk of participants to the group chat via a link in 1:1 chats. Of the 33 accounts , 18 of the accounts represented as female accounts, aged 14-26 and all accounts had a minor female as their profile images. The remaining 12 accounts[2] had a stated gender of male – and five of those had minor females as their profile image. There was no Facebook Group or Page convergence between any of the members of the Group Chat so the method they used to find each other is currently unknown. It should be noted that actor discovery continues to be an ongoing information gap and will be a priority for the ongoing activities following this Taskforce.

Inbox review of the Algeria-based account located 1:1 threads with additional CEI traders who were not present in group chats, with A1 and egregious content.

[1] https://fburl.com/mat2/ia3yscup

[2] Three accounts have been permanently deleted.

Like

Comment

Share

View on Workplace