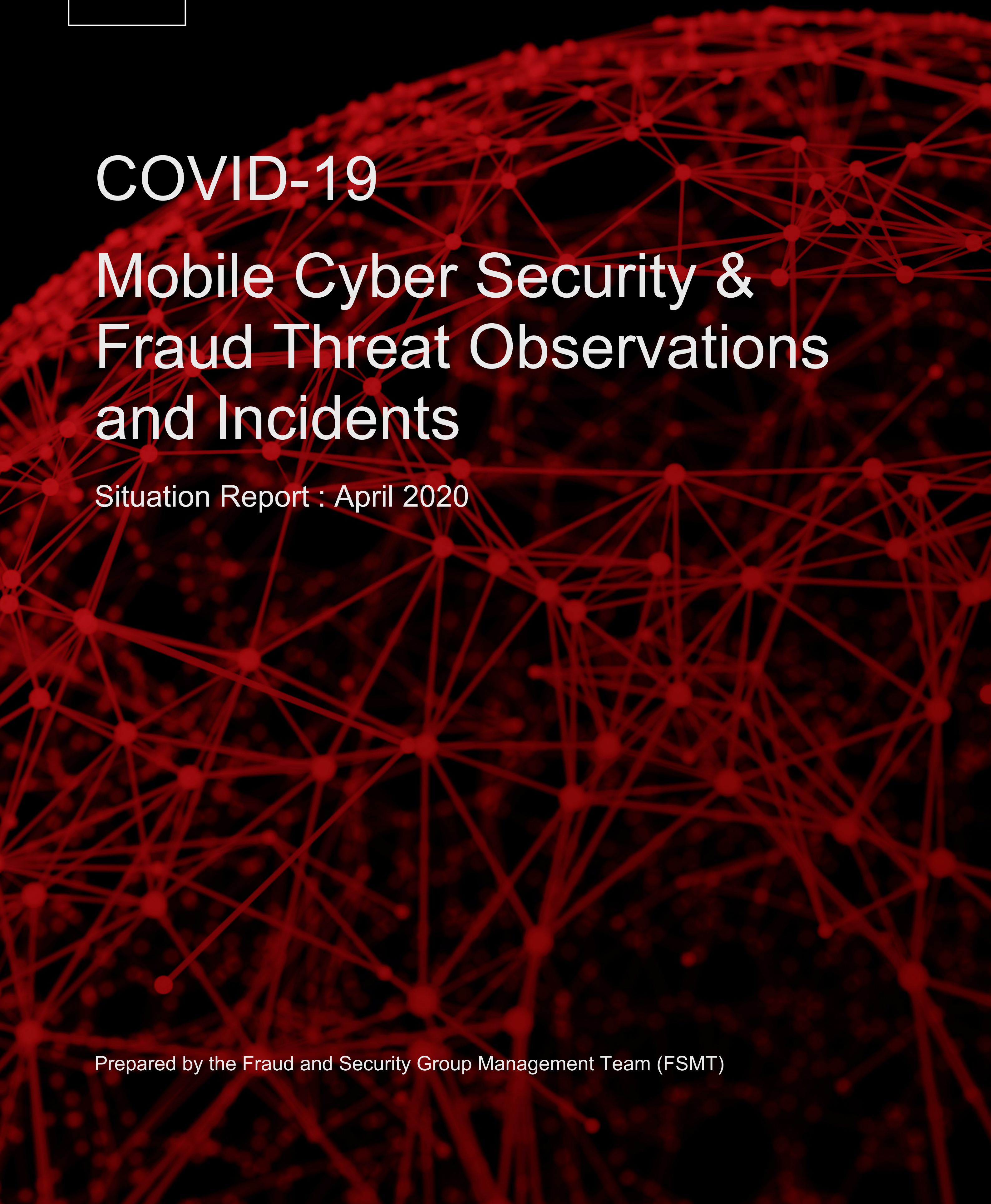


COVID-19

Mobile Cyber Security & Fraud Threat Observations and Incidents

Situation Report : April 2020

Prepared by the Fraud and Security Group Management Team (FSMT)

Contacts:

FASG Chair: david.rogers@copperhorse.co.uk

GSMA Head of Industry Security: jfrance@gsma.com

Member Fraud and Security Intelligence:

Intelligence Submissions: fsc@lists.gsma.com

Structured Cyber-Intelligence Sharing - T-ISAC: t-isac@gsma.com

Table of Contents

Executive Summary

This report has been prepared by members of the GSMA Fraud and Security Group (FASG) management team which comprises the various subject domain sub-group leaders and global region leaders, together with the security leadership in the GSMA staff team.

The report provides a brief outline of mobile-related fraud and security concerns specific to the COVID-19 pandemic. This report covers the March-April 2020 timeframe and is based on open source intelligence, submitted intelligence to the GSMA Fraud and Security Group and other public information including news reports.

Fraud and security issues have been re-targeted towards businesses shifting their practices towards home-working and consumers who are locked down. Campaigns of fraud are shifting towards manipulating consumer concerns and incentives – manipulating commercial, financial and official government outreach campaigns around COVID-19 via SMS and other messaging and voice channels, however it should be noted that due to mobile network operator controls in some countries, there has been little impact of such campaigns in those places. Some types of fraud are naturally decreasing due to the inability for the majority of the world to travel or to buy things in shops, whilst unattended offices have led to a rise in commercial / retail burglaries and PBX (Private Branch Exchange) hacking. With the evidence received, overall, at this current time it appears that fraud remains roughly consistent with normal times, however further work is required to see the knock-on effect of these unprecedented events.

COVID-19 related applications have been the target of copycat malware and spyware, with commercial spyware companies also starting to get involved in contact tracing, seemingly using the mobile network.

Privacy and security concerns around COVID-19 applications have been raised by academics and specialists around the world, with calls for transparency and decentralised methods to be employed for contact tracing. Hackers are starting to focus efforts against Bluetooth, which many apps will use for contact tracing. This is a potential area of risk in the coming months as such apps become more widely spread.

Conspiracy theories spread around 5G and COVID-19 have resulted in base station attacks and on engineers working on installations, particularly in the UK.

Introduction

The following is a summary report of fraud and security issues and considerations encountered by the GSMA Fraud and Security Group members during the COVID-19 pandemic. The report focuses on COVID-19 specific issues but makes observations on existing concerns where appropriate.

The FASG is holding intelligence sharing calls as needed in order that GSMA members can share COVID-19 related security and fraud intelligence. Members are encouraged to share intelligence to both the Intelligence mailing list and to the GSMA's T-ISAC service which provides structured cyber-threat intelligence sharing.

- Intelligence Submissions: fsc@lists.gsma.com
- Structured Cyber-Intelligence Sharing - T-ISAC: t-isac@gsma.com

This document is intended to provide an intelligence summary at the time of writing, and reflects the information available to the authors and contributors. It has not been subject to formal FASG review or approval.

Observations and Incidents

The following observations from the Fraud and Security Group membership have been reported to the GSMA FASG mailing lists, at intelligence calls and through open source information, as well as news reports. References are added where possible. Where appropriate, some information has been anonymised.

It is understood that whilst there is not a general increase in overall cybercrime, the focus has shifted to COVID-19 themed attacks which target consumers and enterprise users who are stuck at home during the lockdown.

Mobile networks are not seeing significant increases in attacks aimed at the mobile infrastructure and security teams are reporting normal levels and types of incidents.

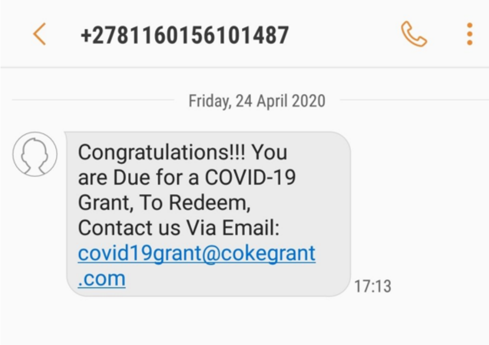
SMS-based Messaging Scams

Across the world, 'Smishing' or SMS phishing campaigns against mobile users have been re-branded with COVID-19 themed messages.

Some examples are shown below. Broadly the messages follow the pattern of:

- Threats of fines for breaking lockdown conditions
- Offers of financial assistance (government, tax authorities, banks)
- Spoofing of government messages
- Contact tracing app related
- Impersonation of companies including mobile network operators
- Sale of non-existent vaccinations against COVID-19 or 'snake-oil' cures

These reflect some existing legitimate attempts by governments and industry across the globe to rapidly assist people. The messages sometimes fake the SenderID. E.g. 'UK_Gov'. The fraudulent messages lead to booby-trapped websites or seek to extract personal information such as a user's bank details.



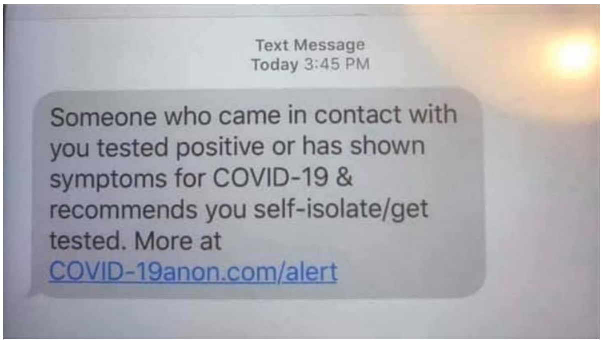
+2781160156101487

Friday, 24 April 2020

Congratulations!!! You are Due for a COVID-19 Grant, To Redeem, Contact us Via Email: covid19grant@cokegrant.com

17:13

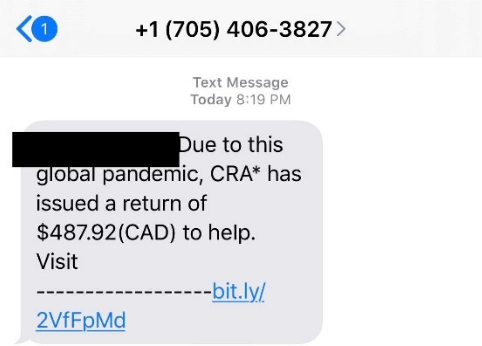
Figure 1 - Example of a smishing message from South Africa (image taken from Twitter: #covid19scamsms)



Text Message
Today 3:45 PM

Someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at COVID-19anon.com/alert

Figure 2 - Example smishing – contact-tracing (image taken from Twitter: #covid19scamsms)



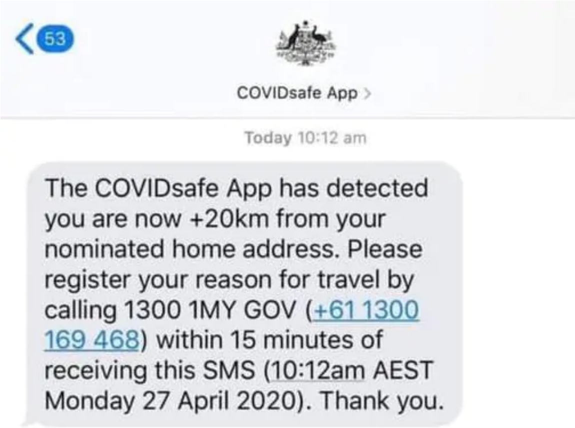
+1 (705) 406-3827

Text Message
Today 8:19 PM

[redacted] Due to this global pandemic, CRA* has issued a return of $487.92(CAD) to help. Visit ------------------bit.ly/2VfFpMd

Figure 3 - Example of offer of financial assistance smishing message from Canada (image taken from Twitter: #covid19scamsms)

Within 24 hours of the Australian COVIDSafe application release, fraudsters were targeting users with scam SMS messages related to it.



The COVIDsafe App has detected you are now +20km from your nominated home address. Please register your reason for travel by calling 1300 1MY GOV (+61 1300 169 468) within 15 minutes of receiving this SMS (10:12am AEST Monday 27 April 2020). Thank you.

Figure 4 - Example of false lockdown breach message, spoofing the Australian COVIDSafe application (image taken from Twitter: #covid19scamsms)

The elderly and vulnerable can be specifically targeted and are particularly susceptible to such scams. Intelligence reports showed users of a mobile network operator being targeted in Argentina with messages purporting to be from the operator.

One GSMA member company reported an increase of around 150% in registered SMS phishing URLs between the middle of March and end of April 2020. The majority of these (over 70%) were COVID-19 related.

Mobile network operators are blocking the originating numbers of the scam messages and phishing sites are being reported and taken down.

Some user guidance has been issued by governments and industry. In the UK and the USA, the use of the 7726 ‘spam’ reporting messaging short code has been promoted.

Fraudsters have regularly adapted their techniques to evade filtering and blocking, for example by using non-standard fonts to represent the hyphen in COVID-19.

In the UK, the Mobile Ecosystem Forum (MEF) has been working with the National Cyber Security Centre (NCSC) to identify and block messages[1].

China’s experience of these types of issues were ever-changing throughout the outbreak period between January and March 2020, with fraudsters reacting to real-world events and issues. Complaints of fraud included:

- Fake offers of air ticket refunds as travel began to be curtailed
- During the lockdown: click farming, gambling related and faked warnings from schools
- False offers of loans as businesses began to open up again

SMS-based messaging scams have had little impact in some countries, in large part because of controls in place by mobile network operators. Two operator groups reported that across the

[1] https://www.mobileuk.org/news/industries-unite-to-tackle-sms-fraudsters-exploiting-covid-19-text-alerts

countries where they operate, they had almost no SMS-scams because they had been able to successfully block the vast majority of attempts by fraudsters.

Email Phishing

Many companies and governments are being affected by email phishing which impersonate their entities in order to dupe users. The elderly and vulnerable can be specifically targeted and are particularly susceptible to such scams.

Intelligence reports show that emails are being sent which impersonate mobile network operators, offering prepaid top-up and post-paid service payment via credit card. Other attacks have included fake bills from mobile operators and fake human resources emails with attachments.

Business Email Compromise (BEC) and ‘whaling’ type scams against senior individuals in companies are understood to have increased, however it has been observed by one mobile network operator that their controls are holding and that attempts have not been sophisticated.

Vishing and Telephone-based scams

Voice phishing has taken place in some countries and is expected to increase as lockdowns continue and more people are stuck at home around the world. In China, fraud call complaints during their period of lockdown included:

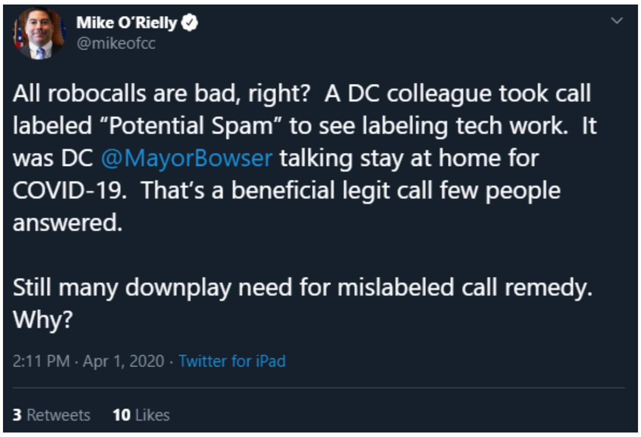
- Impersonating government officers or sales staff in a pharmaceutical research institute
- Selling of counterfeit medicines
- Impersonating staff in a hospital or charity such as the Red Cross, calling for donations
- Falsely claiming that a family member is affected and isolated and hospital fees need to be paid

One operator in Russia observed social engineering of customers via voice calls.

Robocalls

It has been observed that Robocalls have shifted focus to COVID-19 themes, including the offer of testing, protective equipment, loans, working opportunities, etc. are reported to have increased significantly. Operators need to respond quickly and filter and block the originating numbers.

Some governments and local councils have used robocalls to provide COVID-19 messages to citizens. These have in some cases been blocked or mislabelled as spam. Call registries are being setup to eliminate the incorrect spam tagging of legitimate calls.



Mike O'Rielly
@mikeofcc

All robocalls are bad, right? A DC colleague took call labeled "Potential Spam" to see labeling tech work. It was DC @MayorBowser talking stay at home for COVID-19. That's a beneficial legit call few people answered.

Still many downplay need for mislabeled call remedy. Why?

2:11 PM · Apr 1, 2020 · Twitter for iPad

3 Retweets 10 Likes

Figure 5– Commissioner Mike O'Reilly of the US Federal Communications Commission highlights issues around robocalling. Source:

Mobile Malware

Malicious applications with COVID-19 themes have been discovered by mobile security companies[2]. These were not in official app stores, which appear to be successfully avoiding infiltration. Applications identified include some which have been developed based around the Cerberus Android banking trojan 'malware as a service'.

Other apps included premium rate diallers, ransomware, adware and information stealing trojan (RATs), again adapted to fit COVID-19 themes. Spyware is separately covered below.

COVID-19 related advertising in web and mobile applications has been used as channels to lure users to phishing websites. This has seen the abuse of legitimate government and corporate imagery and logos as well as legitimisation by targeting trusted advertising networks such as Google Ads. Mobile network operators are working with these providers to take down fraudulent adverts.

As contact tracing applications become more widely spread, it is expected that mobile malware applications will increase.

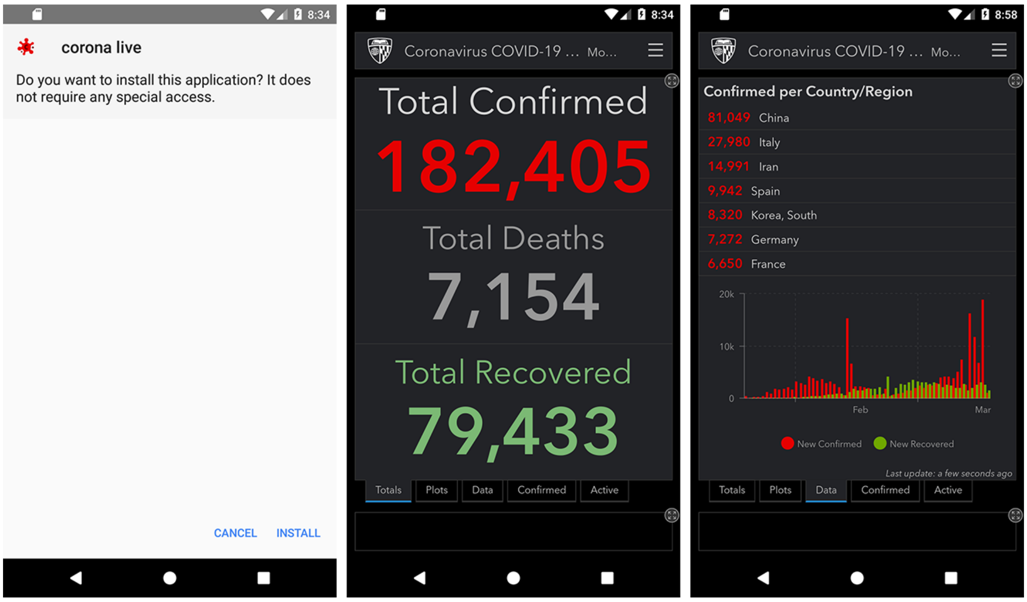
Users are advised to stick to the main app stores and not to side-load applications from websites.

Private / Commercial Spyware

Mobile security company Lookout observed in March that commercial spyware companies were turning their attention to COVID-19[3]. One sample they looked at was a trojanised version of the 'corona live' application, containing the SpyMax spyware. In one case, the spyware appeared to

[2] https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/
[3] https://blog.lookout.com/commercial-surveillanceware-operators-latest-to-take-advantage-of-covid-19

target Libyan mobile users. A number of the apps they have observed share common C2 infrastructure.


corona live

Do you want to install this application? It does not require any special access.

Total Confirmed
182,405
Total Deaths
7,154
Total Recovered
79,433

Confirmed per Country/Region

81,049	China
27,980	Italy
14,991	Iran
9,942	Spain
8,320	Korea, South
7,272	Germany
6,650	France

Last update: a few seconds ago

Figure 6 - Image: Lookout

It was reported in April that NSO Group, an Israeli private spyware company were offering contact tracing. It is possible that this exploits mobile network features rather than targeting devices themselves[4].

Mobile Fraud Observations

Due to the global lockdown, the inability for the majority of the world's citizens to travel and retail largely closed, it has been observed by mobile network operators across the world that the following types of fraud are substantially reduced:

- Roaming fraud
- Subscription fraud
- Handset subsidy fraud
- SIM swap

The following types of fraud have been observed to have increased:

- PBX fraud
- Arbitrage

It remains unclear as to whether other frauds such as International Revenue Share Fraud (IRSF) and SIM box fraud are changed, although traffic to certain countries has been observed to have

[4] https://www.bbc.co.uk/news/health-52134452

increased without explanation. However, the combination of PBX fraud to enable IRSF has seen a marginal upturn, probably because of a lack of presence in physical premises. The increase in PBX hacking risk can also be caused due to increased remote working, companies have extended their VoIP network out of their local networks, connecting remote workers via SIP (Session Initiation Protocol) clients to a corporate PBX. Lack of attention to security in this case makes a SIP server vulnerable.

Mobile network operator data allowance increases and tariff changes have resulted in increased levels of Arbitrage and it has been observed that there is an increased level of roaming data charging bypass.

One mobile network operator observed rising Wangiri attacks in a Balkan state but it is unclear if this was directed specifically because of COVID-19.

It is suspected, but not confirmed that IoT subscription related frauds are increasing which may possibly be because companies are less focused on checking bills and unexpected charges.

In general, as observed with international drugs cartels[5], some fraudsters have had their operations significantly disrupted because of supply chain and movement challenges. This has had a clear beneficial impact in reducing some types of fraud. There is reduced ability for fraudsters to get access to equipment, for example SIM cards and devices. This, combined with their inability to transport goods and the higher likelihood of getting stopped by the Police make committing some frauds more difficult.

In some cases, law enforcement is more active – for example stopping vehicles, but in other areas they have reduced their focus.

Fraud is changing shape with some operators experiencing and uptick in some frauds with a downturn in others and as a whole has not increased and overall fraud continues to be roughly consistent with normal circumstances, despite the global lockdown.

Distributed Denial of Service Attacks (DDoS)

One network operator group reported that they had seen DDoS attacks, combined with ransom demands against healthcare organisations in different parts of the world. They also expect increased attempts at extortion of businesses and individuals, threatening access to remote access and key services.

The Insider Threat

Many companies are adapting rapidly to home-working for their employees. This applies to the individuals too and newer issues related to loss of income may lead to increased fraud risk,

[5] https://www.latimes.com/world-nation/story/2020-04-20/cartels-are-scrambling-virus-snarls-global-drug-trade

especially due to the lack of oversight and monitoring. Procurement fraud risks may also increase in this climate.

In the rush to purchase equipment for staff members there is also the possibility of supply-chain related risks – pre-installed malware on devices, sub-standard or counterfeit devices, plus the deployment on home networks which may already be compromised in a number of ways may lead to business cyber security and fraud issues.

Mobile network operators have observed a substantial reduction in some internal issues such as commission and expenses frauds. However, it has also been noted that the volume of whistle-blower reports received by operators has reduced during the pandemic, largely attributable to the shift to home working and perceived lack of supervisory scrutiny, so network operators should satisfy themselves that any apparent reduction in internal fraud is genuine, and not just an issue that hasn't yet been reported.

Physical Security Threats

Office buildings and retail outlets have been targets of burglaries due to them being empty[6].

Base station attacks (further outlined below) have increased due to disinformation around 5G. At least one of these attacks was on a base station which was having its capacity upgraded to serve a hospital. These represent a resilience, availability and business continuity issue for mobile network operators

Some staff members have been verbally abused and physically threatened while working on mobile network installations. Installation companies have removed company branding from vehicles and staff workwear.

From open source reports and intelligence received from network operators, in Europe targets included: 61 arson attacks in the UK; 80 cases of harassment in the UK; 16 arson attacks in The Netherlands; death threats against a spokesman for the Dutch telecoms coordinator; three incidents of harassment against telco maintenance workers in The Netherlands; three arson attacks in Ireland; at least one arson attack in Belgium, Italy, Cypress and Sweden; one suspected arson attack in Finland; mass mailing targeting MPs and government officials in Bulgaria; mass calls and threats targeting a public authority in Sweden, forcing it to deactivate its phone lines.

[6] https://sanfrancisco.cbslocal.com/2020/04/27/coronavirus-update-san-francisco-police-issue-17-citations-for-health-order-violations-warn-78-others/

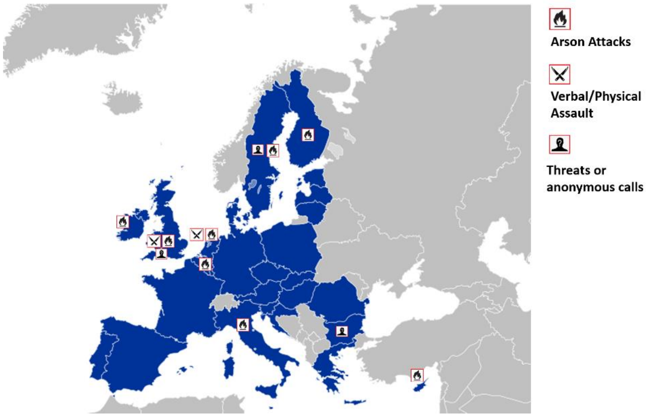


Figure 7 – Incidents and types across Europe

A further five incidents of arson against base stations were noted in South Africa.

5G Disinformation and Attacks

Conspiracy theories around 5G and health have been circulating in Europe for the past 18 months or so but has recently morphed into claims that COVID-19 is being caused by 5G. This has now resulted in physical attacks on base stations. Vodafone in the UK has described this as a "matter of national security". Some of the conspiracies were amplified by the Russian TV station RT, as reported in June 2019 by Wired[7] and then further amplified by other TV stations such as Fox News in the US.

Figure 8- Graffiti with 5G / Covid-19 conspiracy theory

[7] https://www.wired.co.uk/article/5g-health-risks-concerns

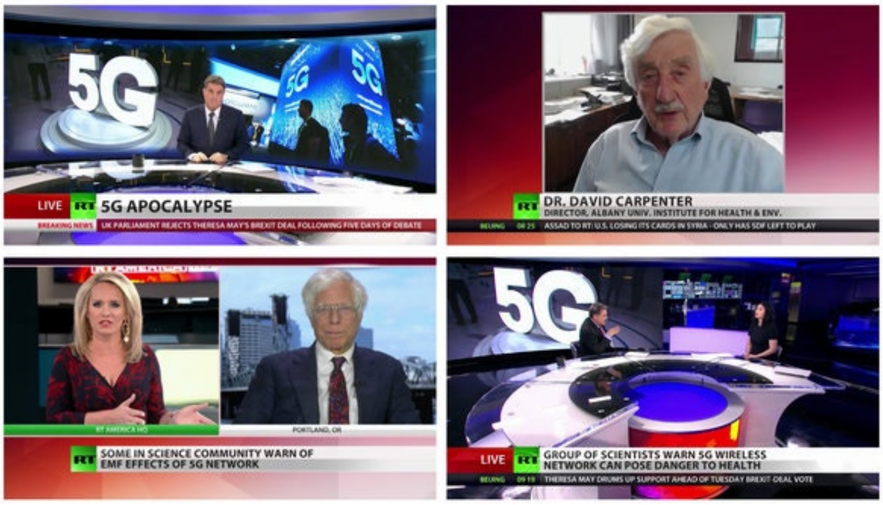

5G
LIVE
RT
5G APOCALYPSE
BREAKING NEWS
UK PARLIAMENT REJECTS THERESA MAY'S BREXIT DEAL FOLLOWING FIVE DAYS OF DEBATE
DR. DAVID CARPENTER
DIRECTOR, ALBANY UNIV. INSTITUTE FOR HEALTH & ENV.
ASSAD TO RT: U.S. LOSING ITS CARDS IN SYRIA - ONLY HAS SDF LEFT TO PLAY
PORTLAND, OR
SOME IN SCIENCE COMMUNITY WARN OF EMF EFFECTS OF 5G NETWORK
GROUP OF SCIENTISTS WARN 5G WIRELESS NETWORK CAN POSE DANGER TO HEALTH
THERESA MAY DRUMS UP SUPPORT AHEAD OF TUESDAY BREXIT DEAL VOTE

Figure 9- 5G disinformation promoted by Russian TV station RT.

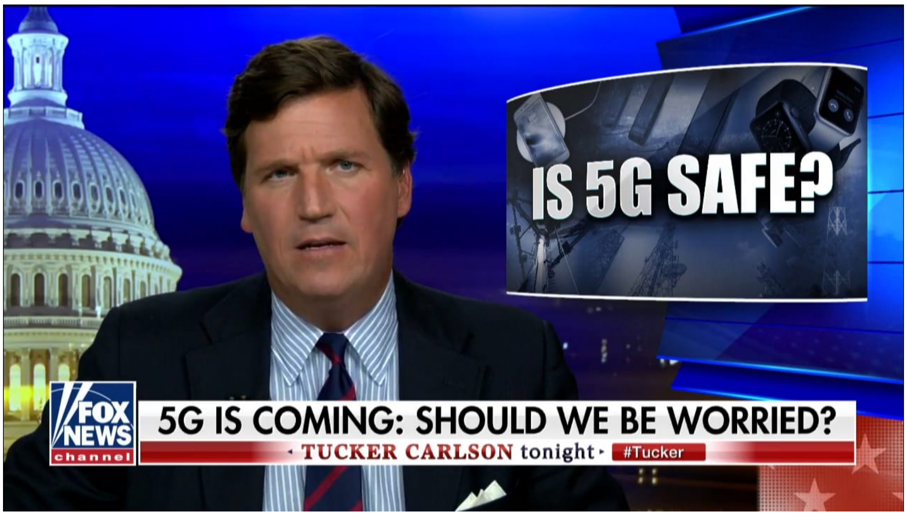


Figure 10 - Amplification of 5G Disinformation in the USA

Base Station Attacks

There has been a number of attacks on base stations around the world, including cables being hacked out of the masts through to petrol being poured in and around the equipment and then being set alight.

Base station on fire.

The UK has appeared to be a particular focus for these attacks with occurrences across the country. Other examples are widespread including in New Zealand[8], The Netherlands[9] and Ireland[10]. Mobile UK reported that there were 20 attacks across the Easter weekend (10th-13th April 2020)[11]. By the 25th of April, the West Midlands of the UK was reported to have had 38% of all UK attacks, which totalled 53[12].

Base stations servicing hospitals were attacked in Birmingham, UK and Letterkenny, Ireland[13].

In the vast majority of the cases, the base stations were not 5G infrastructure.

Some staff members have been verbally abused and physically threatened while working on mobile network installations. Installation companies have removed company branding from vehicles and staff workwear.

Disinformation Campaign

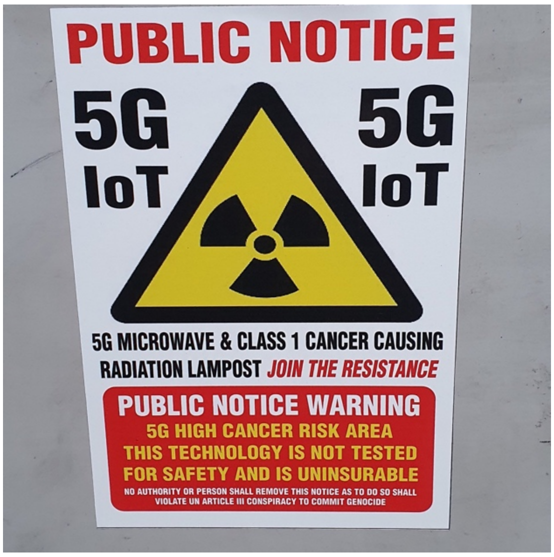
5G conspiracy theories around health have been around for a while, as they have been on previous generations of technology (including the introduction of electricity and the railways!), but

[8] https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12324501
[9] https://www.dw.com/en/5g-protesters-sabotage-dutch-phone-towers/a-53094033
[10] https://www.independent.ie/irish-news/coronavirus-ireland-5g-arsonists-target-mobile-masts-as-conspiracy-theories-start-to-take-their-toll-39124082.html
[11] https://www.bbc.co.uk/news/technology-52281315
[12] https://www.expressandstar.com/news/health/coronavirus-covid19/2020/04/25/twenty-5g-masts-attacked-in-west-midlands/
[13] https://www.independent.ie/irish-news/coronavirus-ireland-5g-arsonists-target-mobile-masts-as-conspiracy-theories-start-to-take-their-toll-39124082.html

as mentioned above, these appear to have been nurtured and have been merged with the COVID-19 pandemic, which has its own set of conspiracy theories on its own.

From a cyber-security perspective, it appears that organised campaigns are taking place across social media which are fanning the flames, resulting in increased action in the physical world. Given the actions of some nation states around fake news and other disinformation in recent years, it is entirely possible that state actors are involved.

Posters and stickers have appeared in towns and on mobile infrastructure in public places in the past year or so, whilst conspiracy theorists like David Icke have been given the oxygen of publicity on major platforms online and on television, resulting in complaints to telecoms and media regulators.



PUBLIC NOTICE

5G IoT 5G IoT

5G MICROWAVE & CLASS 1 CANCER CAUSING RADIATION LAMPOST JOIN THE RESISTANCE

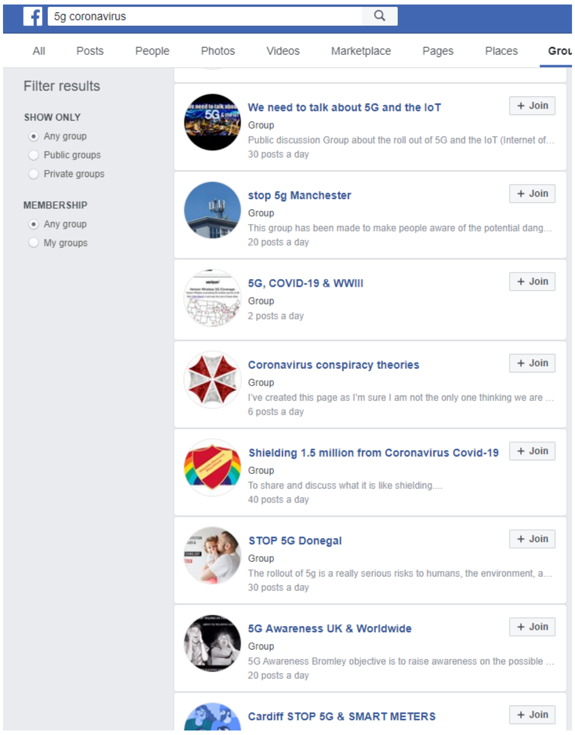
PUBLIC NOTICE WARNING

5G HIGH CANCER RISK AREA
THIS TECHNOLOGY IS NOT TESTED
FOR SAFETY AND IS UNINSURABLE

NO AUTHORITY OR PERSON SHALL REMOVE THIS NOTICE AS TO DO SO SHALL VIOLATE UN ARTICLE III CONSPIRACY TO COMMIT GENOCIDE

Figure 11 - A sticker posted in Glasgow, UK during April 2020.

While social media companies are taking action, a quick search quickly reveals that there are still many groups and individuals promoting the conspiracy theories.



We need to talk about 5G and the IoT
Group
Public discussion Group about the roll out of 5G and the IoT (Internet of...
30 posts a day

stop 5g Manchester
Group
This group has been made to make people aware of the potential dang...
20 posts a day

5G, COVID-19 & WWIII
Group
2 posts a day

Coronavirus conspiracy theories
Group
I've created this page as I'm sure I am not the only one thinking we are ...
6 posts a day

Shielding 1.5 million from Coronavirus Covid-19
Group
To share and discuss what it is like shielding....
40 posts a day

STOP 5G Donegal
Group
The rollout of 5g is a really serious risks to humans, the environment, a...
30 posts a day

5G Awareness UK & Worldwide
Group
5G Awareness Bromley objective is to raise awareness on the possible ...
20 posts a day

Cardiff STOP 5G & SMART METERS

Figure 12 - Social media groups and individuals promoting conspiracy theories

In the UK, social media companies had a meeting with the government to agree to take down the disinformation campaign, videos and other material[14].

Traffic Pattern Changes and Threat Detection

There is widespread reporting of significant changes in usage volumes and patterns both within mobile[15] and fixed line communications[16]. Operators are seeing significant volume increase both in data and voice, with domestic usage patterns shifting towards the day away from the evening and business traffic abating due to remote working. Typical usage, such as call lengths are also changing. Some machine-learning assisted fraud and security threat detection tools utilise pattern recognition, and due to pattern changes have become less reliable and need to be 're-trained' to attain previous efficacy levels.

Remote Access Infrastructure

Businesses have moved aggressively and rapidly to enable their workforces to be able to remote work as a business continuity response to movement restrictions. There have been reports of attackers trying to compromise VPN concentrators to gain access to corporate networks and

[14] https://www.bbc.co.uk/news/technology-52172570
[15] https://www.fiercetelecom.com/telecom/spanish-carriers-see-a-40-spike-network-traffic-due-to-covid-19
[16] https://www.techrepublic.com/article/data-visualizations-show-internet-usage-in-inner-cities-idled-by-covid-19/

assets. As with any rapidly deployed infrastructure / services that may not have been afforded a full test and evaluation period, there is a possibility of misconfiguration and other issues that leave such avenues vulnerable and open to compromise

COVID-19 Contact-tracing

Mobile Network Data

Mobile network operators have been requested by governments across the world to provide information on subscribers. In some cases, this data is anonymised, in other cases not, depending on jurisdiction.

Contact Tracing Applications

Concerns are being raised by academics and privacy specialists on the potential for abuse for contact tracing applications[17]. There have been calls for full transparency of the source code used for such applications. Singapore's TraceTogether has been open sourced[18] and other countries have based their applications on Singapore's work.

In the rush to develop contact tracing and COVID-19 applications, there is significant risk of the introduction of flaws which could be exploited once deployed. A comprehensive list of COVID-19 applications is being maintained on Wikipedia[19].

Google and Apple worked together to offer APIs to developers which allow for anonymous collection and transmission of contacts.

A letter written by 200 academics worldwide appealed for security and privacy, transparency and decentralisation in any application development[20]. Professor Ross Anderson at the University of Cambridge and others have raised concerns about the accuracy of Bluetooth – there is evidence to show that there will be a high number of false positives (i.e. people who were not within a physically dangerous position to infect a user). The false negatives issue is the bigger problem however (people who were in a position to infect a user but that were not recorded). GSMA is involved in cross-industry efforts to assist in increasing the performance and accuracy of Bluetooth data based on the calibration for particular types of devices, with the work expected to be complete by the end of May 2020.

Despite all the concerns however, it is clear that a mobile application with this kind of capability is one part, albeit a small one, of assisting in contact tracing and helping to lift lockdown measures across the world.

[17] https://ncase.me/contact-tracing/
[18] https://github.com/opentrace-community
[19] https://en.wikipedia.org/wiki/COVID-19_apps
[20] https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view

Australia launched its COVIDSafe application in late April 2020 which quickly received millions of downloads.

Open questions remain about the long-term uses of the technology. The general expectation in democratic countries is that such invasive and draconian measures should be in place for a time-limited period. Transparency is key and mobile companies should make every effort to retain the confidence of their users that the trust they are placing in them now is not abused once a vaccination is widely deployed and emergency conditions are lifted across the world.

Bluetooth

Hackers are showing increased interest in Bluetooth LE. Contact tracing applications may require Bluetooth to be turned on when users leave their homes.

On April 22nd 2020, a CVE was issued for a vulnerability in Android 8 and 9 which could result in a zero-click remote control execution exploit called BlueFrag[21]. The researchers were able to also exploit Android 10 which an adaption of their attack.

Whilst the global device estate is not a homogenous attack surface, there are significant commonalities which increase the potential impact of a successful exploit – a duopoly of mobile operating systems, common contact tracing applications for mass populations and a significant number of operational, older devices in the field. This is of particular concern for older devices where there may be no patch issued for discovered vulnerabilities.

Other (non-mobile specific)

Zoom-bombing

There has been increased targeting of video-calling services, such as Zoom. This attack is known as ‘Zoom bombing’. The companies providing these services have increased security accordingly and are providing users with advice on how to secure their video calls.

Adoption of Digital Distance Tooling and Inexperience

As mentioned in the Insider Threat section, many people and businesses are adopting new digital tools both socially and professionally and are not familiar with functionality and configuration. This gives rise to the opportunity for an attacker to exploit such inexperience or misconfiguration and / or the lack of application and use of security measures. Such inexperience is presenting an opportunity to attackers to exploit such as eavesdropping / personal data collection that could lead to service account takeovers or used in secondary attacks and compromise. Some service providers are now changing default configurations to enable security features by default (such as

[21] https://insinuator.net/2020/04/cve-2020-0022-an-android-8-0-9-0-bluetooth-zero-click-rce-bluefrag/

passcodes on video conference sessions[22]) and running education campaigns to highlight how to use tools and protect themselves online.

As the numbers of tools in use proliferate it is also likely that poor digital hygiene will result in significant re-use of credentials and a compromise in one service may lead to compromise in others, SpyCloud has calculated a 74% rate of password reuse among Fortune 1000 Telecom employees (the highest of all 21 industry verticals in the F1000).

Authority Chains and Business Processes

Business processes in many cases have had to rapidly change to support remote working, and in many cases the normal authorisation processes, levels and personnel have changed, opening an opportunity for exploitation if weakened either through poor design or through inexperience. Whaling, Business Email Compromise[23] and invoice frauds are obvious attack vectors that could be used to exploit such situations. Alongside these changes many business support functions (including IT and Information Security) have also moved to operate remotely and the distancing of such has potentially weakened the support and capability that business functions rely on to protect / mitigate issues.

[22] https://betanews.com/2020/04/04/zoom-security-meeting-passwords-virtual-waiting-rooms/

[23] https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

Summary

The Fraud and Security Group is made up of thousands of individuals working for mobile network operators and companies from the mobile ecosystem from around the world. As such, it is the focal point for the world's experts in mobile fraud and cyber security.

Its management group, the GSMA Fraud and Security Management team (FSMT), will continue to facilitate incident and intelligence sharing amongst members.

At the end of April 2020, it is the FSMT's assessment that overall fraud and security issues are not observed to be rising, however the prime focus of attackers, cyber-criminals and fraudsters is COVID-19, in order to take full advantage of the unprecedented situation the world finds itself in.

FASG intelligence sharing calls are taking place as needed with members from around the world. Members are also sharing data and information via a dedicated intelligence sharing mailing list. Cyber threat intelligence and Indicators of Compromise (IOCS) are also being shared via GSMA's T-ISAC service[24] which members are encouraged to join and contribute to.

Members of the group are also involved in other initiatives such as the CTI-League[25] and cyber threat intelligence has been shared to the Fraud and Security Group from external individuals and groups researching cyber security threats around COVID-19. This has all been acted upon and shared. A further update to this report will be issued for the month of May 2020.

The FSMT is grateful to all who have contributed to this initiative and the intelligence in this report, but thanks must go to the millions of healthcare professionals around the world who are working tirelessly to assist victims of COVID-19.

Stay Home, Stay Safe.

If you find any errors or omissions, please contact us with your comments. You may notify us at fasg@gsma.com

[24] https://www.gsma.com/security/t-isac/
[25] https://cti-league.com/

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com