An NCC Group Publication

Cyber Threat Advisory COVID-19

Written by
Ian Usher & Matt Hull

Contents

COPYRIGHT AND CONFIDENTIALITY STATEMENTS

The information in this document is subject to change without notice. NCC Group shall not be liable for any damages resulting from technical errors or omissions which may be present in this document, or from use of this document.

This advisory provides insight into Threat Actor behaviour and motivations and some of the campaigns that have emerged under COVID-19.

It also seeks to help you as individuals or as part of a wider business or organisation, to navigate your way through the situation in a secure and resilient manner.

1. Overview

The world is currently experiencing an unprecedented situation in terms of the scale, reach and impact of COVID-19. Citizens are in lockdown, many businesses are struggling financially; it has touched us all in one form or another.

It is usual for Threat Actors to take advantage of major events, exploiting them to either make a profit or use them as an opportunity to steal information. For example, there have been numerous attacks on high profile events such as the Olympic Games, including the Athletes' data hack in the Winter Olympics in 2018. There are also annual trends in phishing activity at commercial or religious dates such as Black Friday or Diwali.

It is usual for Threat Actors to take advantage of major events, exploiting them to either make a profit or use them as an opportunity to steal information.

The proliferation of disinformation and so-called 'fake news' is also noticeable in the wake of a major event or incident. This can lead to an increase in fear, uncertainty, and doubt (FUD) among populations, and often results in panicked responses of one form or another.

These circumstances provide Threat Actors a perfect opportunity to develop social engineering campaigns. Social engineering is essentially the art of manipulating people so that they reveal private information or do something that they wouldn't ordinarily do. In the context of cyber-criminality, these campaigns are usually launched with a view of manipulating people to reveal passwords, banking information, or provide access to their computer or mobile device. Therefore, it is unsurprising that Threat Actors have been taking full advantage of the global COVID-19 pandemic. These campaigns range from the sophisticated and well thought-out, to the rushed and blatant attempts to capitalise on fear.

This advisory provides insight into Threat Actor behaviour and motivations and some of the campaigns that have emerged under COVID-19.

It also seeks to help you as individuals or as part of a wider business or organisation, to navigate your way through the situation in a secure and resilient manner.

Executive summary

Executives and business leaders will no doubt be facing multiple challenges at this time, and highly motivated cyber threat actors are potentially one of them. Throw in the potential for staff shortages, and technology challenges hampering business operations, it is a testing time.

Overcoming these challenges while maintaining operational effectiveness and resilience is a priority for all, and one way in which businesses have sought to address these is by implementing far reaching opportunities for employees to work from home. While this approach most definitely has its benefits, it has the potential to introduce vulnerabilities from a cyber security point of view.

In order to mitigate risk from cyber incidents during this crisis, and indeed at any other time, business leaders should ensure that colleagues have the necessary equipment and know how to use it securely. Their IT Help Desks, security incident reporting, and investigation processes should ideally be geared-up towards remote operations. It is likely that help desks will be busier than normal, with people who don't usually work from home getting to grips with their new ways of working. And finally, ensuring that their organisation issues appropriate communications about working securely, and being extra vigilant for the likes of phishing and social engineering.

2. Campaigns

We have divided the type of campaigns we have identified into two categories, Indiscriminate and Targeted campaigns.

Indiscriminate Campaigns

Indiscriminate campaigns are carried out with the intention of impacting as many users as possible. One example is the distribution of phishing emails using mailing lists that have been created by collecting email addresses from breached credential databases.

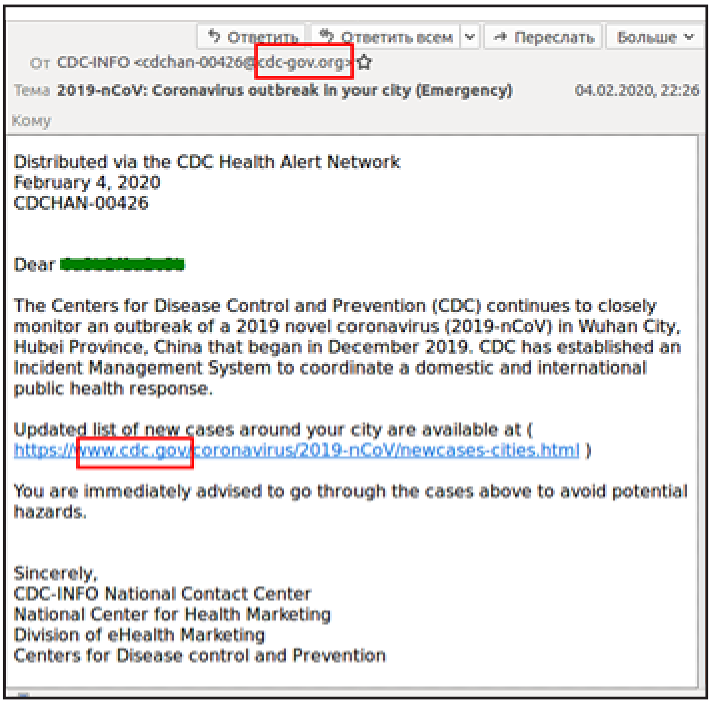
Phishing

Threat Actors have sought to exploit the growing public and media interest in COVID-19 with a number of phishing attacks. Phishing is a common attack vector used to gather information or credentials to support later attack stages. The attacker will typically create an email and supporting infrastructure such as a typo squat domain, which mimics a legitimate organisation.

As the seriousness of the spread of the pandemic became apparent, reports of COVID-19 themed phishing campaigns began to grow. For example, between 26th and 27th March, Risk IQ identified 265,952 spam emails in their spam box feed that contained either "corona" or "covid" in the subject line. [1] Domain Tools have released a list of over 80,000 domains containing terms linked to the pandemic.

Organisations that are directly involved in the COVID-19 response, such as The World Health Organisation (WHO) and the US Centre for Disease Control (CDC), were some of the first to be abused by phishing campaigns. This prompted warnings from these organisations with WHO even highlighting some of the malicious domains such as who[.]com, who[.]org and who-safety[.]org.

An example phishing campaign is below:



От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема 2019-nCoV: Coronavirus outbreak in your city (Emergency) 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

(Source: https://ui.threatstream.com/campaign/60704)

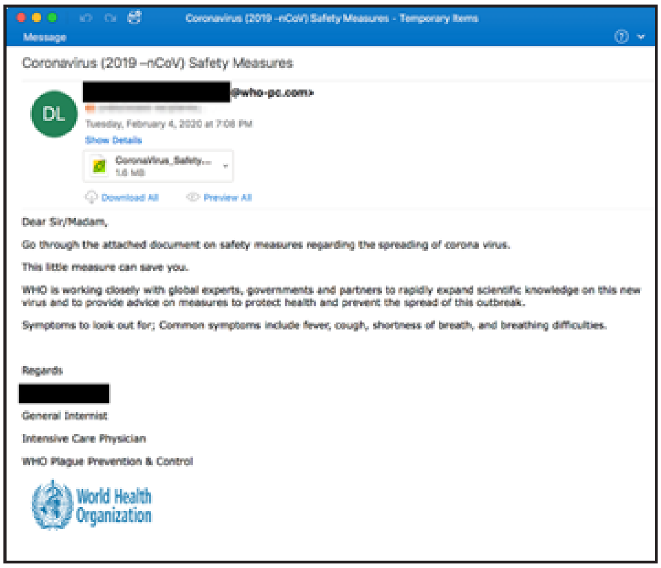
Malspam Campaigns

There has also been a notable increase in malspam campaigns using COVID-19 as a lure. One of the first campaigns identified involved Threat Actors distributing the Emotet banking trojan to Japanese users via a word document. [2]

As Emotet has typically targeted North America and Europe, the targeting of Japan is an interesting departure and signals how responsive Threat Actors are being during the COVID-19 crisis.

While targeted ransomware continues to blight organisations there are also continued efforts by Threat Actors to distribute ransomware indiscriminately through malspam campaigns.

One such campaign was reported on 24th March 2020, in which the mailing list included hospitals in Spain. The emails were reported to Spanish authorities. They contained attachments claiming to provide information relating to COVID-19 but they actually contained Netwalker Ransomware.[3] An example of one of these malspam campaigns can be seen below.



Coronavirus (2019 –nCoV) Safety Measures - Temporary Items

Message

Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety...
1.6 MB

Download All   Preview All

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

World Health Organization

(Source - https://ui.threatstream.com/campaign/60704)

With such a high volume of COVID-19 themed applications available, it is difficult for users to identify what applications are legitimate and what is potentially malicious.

Mobile Phone App Campaigns

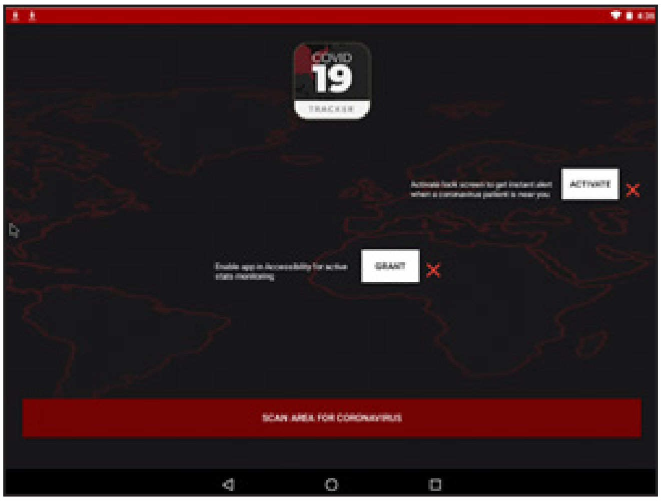
Researchers have identified a growing collection of malicious apps, especially on the android operating system. Whereas Apple OS requires all applications to be installed via the App Store, Android applications can be installed either through the Google Play store or by downloading Android Application Packages (APK).

Even with oversight by Google, the Google Play store still contains a high proportion of malicious applications.[4] These applications can allow an attacker to install malware providing access to information from the victim's phone, keylogging for passwords and access to media stored on the device.

We have identified multiple reports of websites offering downloads of COVID-19 materials containing malware. In one example a Threat Actor created a website that lured users into downloading an Android application under the guise of a COVID-19 heat map, the application (pictured to the right) contained ransomware.[5]

According to a BitDefender report there have been almost 600 applications that contain COVID-19 key words since the 1st January. The majority were not malicious but 9 were classified as Trojans and 10 as Riskware.[6]

With such a high volume of COVID-19 themed applications available, it is difficult for users to identify what applications are legitimate and what is potentially malicious. Another risk from these applications is their potential for spreading misinformation, which will be discussed later in this report.



Activate lock screen to get instant alert when a coronavirus patient is near you

Enable app in Accessibility for active stats monitoring

(Source - https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware)

There have been several reports of NHS staff targeted for their name badges, which are required to gain entry to the supermarkets.

Targeted campaigns

Targeted campaigns refer to operations carried out by Threat Actors where a specific organisation or sector is identified as the preferred victim.

Capitalising on Support for Essential Workers

A number of organisations are providing support to frontline COVID-19 responders such as offering free products or making special concessions to accommodate special needs (e.g. NHS-only shopping hours at supermarkets).

Unfortunately, these concessions have been targeted by criminals. There have been several reports of NHS staff targeted for their name badges, which are required to gain entry to the supermarkets.

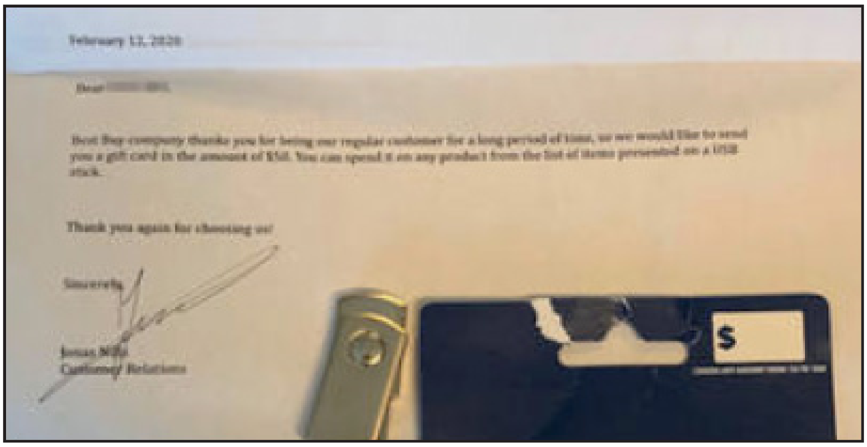
Cyber criminals could also capitalise on organisations publicising their support to COVID-19 responders.

The picture below is an example of a manual method of infecting systems by posting an infected USB stick.[7]

This particular example is not explicitly linked to COVID-19. However it was sent to a hospitality provider many of whom are providing rooms to COVID-19 responders where travel or returning home is not possible.

Advanced Persistent Threat (APT) groups have been known to target hospitality providers to gain information on customers. In the example above the attack was attributed to the financially motivated group known as FIN7 who are known for targeting US retail, restaurant and hospitality sectors.

While this does not appear to relate to COVID-19, the method could be replicated. While additional support or gifts are undoubtedly valued at this time, they should also be treated cautiously.



February 13, 2020

Dear [redacted]

Best Buy company thanks you for being our regular customer for a long period of time, so we would like to send you a gift card in the amount of $50. You can spend it on any product from the list of items presented on a USB stick.

Thank you again for choosing us!

Sincerely,

Jonas Mills
Customer Relations

(Source - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/would-you-exchange-your-security-for-a-gift-card/)

APTs Targeting Political Targets

Malwarebytes researchers identified APT36 launching a COVID-19 themed spear phishing email, designed to impersonate communications from the Indian government, that contained a link to a malicious document. APT36 is believed to be a Threat Actor group based in Pakistan. The malicious document downloaded via the link in the email contained Crimson Remote Access Trojan (RAT).[8]

During the same period, there were reports that Vicious Panda, a Chinese Threat Actor, had launched a similar campaign targeting Mongolia with a fake Government announcement from the Mongolian Ministry of Foreign Affairs. The attached document was supposed to contain COVID-19 spread data from China, however opening the document triggered an infection chain delivering a RAT.[9]

Ransomware operators are not the only Threat Actors actively targeting the healthcare sector. Advanced Persistent Threat (APT) groups are also likely to be targeting COVID-19 research under direction of their various nation states.

Healthcare and Medical Research

The healthcare sector has been routinely targeted by ransomware operators for many years. Due to the critical nature of the services they provide they are an obvious target to threaten with disruption because there is a potential human cost associated with the impact of loss of service.
It seems that for some ransomware operators the human cost of their malicious activities is too much even for them. A blog post by Digital Shadows shows that they have observed some positive messages attempting to dissuade others from attempting to profit from the pandemic, expressing solidarity with impacted countries and even sharing health and safety advice.

Despite these attempts, Brno University Hospital in the Czech Republic was hit by cyber-attack on 12th and 13th March resulting in severe service disruption requiring transfer of patients. Brno University Hospital is one of the largest COVID-19 testing laboratories in the country. At this stage no further details are available but initial reports suggest that this could have been a ransomware attack.[10]

This is not an isolated case. We have also observed multiple reports from Spain of hospitals being targeted with ransomware. Reports highlight that medical centres have been receiving a stream of emails that offer information on COVID-19 but the attached PDFs contain Netwalker ransomware.[11]

There are also reports that the Champaign Urbana Public Health District (CHUPD) in the US was also the victim of a ransomware attack using Netwalker.[12] A COVID-19 themed attachment containing Netwalker Ransomware has been identified by MalwareHunterTeam[13] and uploaded to VirusTotal[14] ; it is currently showing a detection ratio of 31/59.

Netwalker ransomware is also known as MailTo ransomware; it was the subject of an advisory published by the Australian Cyber Security Centre (ACSC) in February 2020 following multiple ransomware incidents.[15] Netwalker ransomware operators have adopted a Big Game Hunting tactic focusing on targeting enterprise networks to maximise the potential pay-out they will receive.

We have also identified reports of a ransomware attack on Hammersmith Medicines Research in the UK. On this occasion it is believed to have been carried out by the Maze ransomware group, the Threat Actors published a notice stating that they had carried out the attack on the 14th of March. The research centre assisted in the development of Ebola and drugs to aid in the treatment of Alzheimers but it is unclear whether they are directly supporting research into COVID-19 at this stage.[16]

Ransomware operators are not the only Threat Actors actively targeting the healthcare sector. APT groups are also likely to be targeting COVID-19 research under direction of their various nation states. Researchers from FireEye have recently released a paper highlighting a global campaign by the Chinese actor designated as APT41.

They identified a global campaign which is believed to have started on 10th January targeting a wide range of sectors including banking, government, healthcare, education, pharmaceutical and telecommunications.[17]

It is highly likely that COVID-19 research will be a top priority for their cyber espionage activities as the Chinese government continue to battle this pandemic.

Finance and Retail Sectors in the Crosshairs

According to the National Fraud and Cyber Crime Reporting Centre, COVID-19 related fraud has increased by 400%.[14] The majority of these cases were either linked to online shopping fraud or phishing.

Finance

Threat Actors are looking to exploit the increased reliance on online banking; those unfamiliar with the practice of using online banking are at a much greater risk of phishing emails mimicking banking organisations. The primary risk to the finance sector, particularly banking, is through the constant barrage of phishing emails, SMS messages and malspam being distributed to customers. We have seen financial malware gangs target specific populations during the early stages of the outbreak.

Trojans such as Emotet and TrickBot were distributed to Japan and Italy as the populations went into lockdown. The operators of TrickBot, for example, were observed removing the majority of targets from the configuration files and solely adding Italian banks to the target list.[18]

As uncertainty in the markets continues and concerns of another recession grows, we are seeing a great deal of reporting on government financial stimulus packages. We expect that this will result in increasing Social engineering by Threat Actors looking to exploit individuals and organisations who are looking to take advantage of this financial assistance.

Retail

The retail sector is one of the sectors that has been hit the hardest by the pandemic. Many high street stores are already in a precarious financial position, prompting those without an established online presence to enter the online marketplace more quickly than would be considered orderly. While this may present the retailer with opportunities to maintain their business, it may also provide Threat Actors with attack opportunities.

The threat for customers is also increasing. The high demand and increased scarcity of household essentials plays right into the hands of Threat Actors. This demand can be exploited through fake advertising banners with links to malicious webpages, fraudulent sales or even denial of service attacks.

The reliance on online shopping infrastructure and the high demand creates something of a perfect storm for Threat Actors with malicious intent. The media coverage of the growing COVID-19 pandemic certainly played a part in the panic buying that caused so much disruption during the early stages of the outbreak, but the spread of misinformation was another contributing factor.

Ransomware operators are not the only Threat Actors actively targeting the healthcare sector. Advanced Persistent Threat (APT) groups are also likely to be targeting COVID-19 research under direction of their various nation states.

3. Avoiding Disinformation

In short, the best way to tackle disinformation is to corroborate what you read online.

Check if the same information is available from a reputable source. Most importantly, if in doubt, don't spread it further.

Disinformation can spread quicker than the virus itself, and while it does not directly affect health, it can be just as damaging in a social context.

Predictable, albeit panicked responses to COVID-19, have triggered unusual behaviour from people all across the globe in pursuit of protecting their families and loved ones. Some of the most common reporting throughout March included people panic buying in supermarkets, while images of empty shelves and people fighting in stores was commonplace.

In one particularly extreme example of this, video footage of shoppers amassing outside an Aldi store in Haarlem, Amsterdam, was widely circulated. These sorts of videos have the ability to incite panic as they have an implied immediacy, and are quickly spread via social messaging applications such as WhatsApp or other social media networks like TikTok.

The investigative journalism group Bellingcat[19], was quick to debunk the video, which had over 400 million views on TikTok alone having been posted at the end of February. The video, had actually been uploaded to YouTube in 2011, nine years before the COVID-19 pandemic.

Whilst there remains uncertainty, the natural hunger for information means that people are generally more open to believing a wider array of news sources. Some of the concerns with the types of disinformation currently circulating include stoking the fires of xenophobia, encouraging selfish behaviour, and casting doubt on nations' measures to protect the population. Perhaps most concerning of all is the potential implications of false medical advice including potential cures, suggestions that certain groups in society don't need to be concerned about the virus or that, in some cases, people should actively try to become infected.

As already mentioned, this FUD amongst people provides an opportunity for criminal entities to capitalise on the situation. The case above is just one example of a number of disinformation campaigns that have circulated since the beginning of the pandemic.

Below are some of the other trends that have been observed by NCC Group:

- Information regarding fake cures and COVID-19 treatments spread via multiple social media profiles and being sold directly on a number of websites.[20]
- Videos of military vehicles and personnel circulating across social media and messaging platforms which insinuate military control is imminent.[21]
- Several nations have made false claims as to the source of COVID-19. A Chinese Ministry official initially stated on social media that the virus was made in a US military lab. Further suggestions out of China later stated that the virus originated in Italy .
- Several conspiracy theories regarding the deliberate release of the virus in order to reduce the world population or manipulate the economic climate have been disseminated.[23] [24]

In short, the best way to tackle disinformation is to corroborate what you read online.

Check if the same information is available from a reputable source. Most importantly, if in doubt, don't spread it further.

Disinformation can spread quicker than the virus itself, and whilst it does not directly affect health, it can be just as damaging in a social context.

4. Mitigation and support

Stay safe and stay well. We will continue to monitor the landscape and keep you informed of any future threats, and offer support and advice.

Navigating this quagmire of threats might feel like a daunting challenge, but it doesn't need to. Following long-standing, basic security advice, and keeping well informed about the changing threat landscape will go a long way to keeping you or your businesses safe online.

As we have seen, the most common attack vector is through malicious emails. With so many employees working from home, there is increased reliance on email and messaging apps. The combination of a comfortable home environment and a higher volume of electronic communication is likely to increase the risk of successful phishing attacks.

As the enforced period of home working continues, we expect to see an increase in successful phishing attacks. To combat this, we recommend that you continue to highlight the risks of phishing, provide examples from current phishing campaigns as examples of what to look out for and detail how to respond to suspected phishing emails.

As we have highlighted, a higher volume of electronic communications is a risk factor. We recommend that any information regarding phishing is shared via a central intranet page or discussed in team conference calls.

Make the most of a decreased workload (where applicable) and focus on enhancing cyber security and resilience. Enable two-factor authentication wherever possible. Identify single points of failure in processes so that vital work can continue in the event of illness.

Encourage employees to use a centralised and regularly updated COVID-19 internal web page. This will reduce employees searching for their own sources and potentially coming across a malicious email or website and it will also help to control the spread of misinformation.
The NCC Group SOC Threat Intelligence Team in conjunction with our Threat Intelligence Fusion centre is continuing to monitor new campaigns and continue to add to our collection of Indicators Of Compromise (IOCs) to aid in detection of these threats against our customers.

NCC Group is hard at work to provide additional support and protection to organisations during this time. The following articles will provide further details and advice:

- Be Remote Ready (https://newsroom.nccgroup.com/news/number-beremoteready-q-and-a-with-ncc-groups-ciso-dominic-beecher-397449)
- Operational resilience (https://newsroom.nccgroup.com/news/updating-your-business-resilience-plan-advice-for-those-concerned-about-covid-19-395707)
- SOC Support (https://newsroom.nccgroup.com/news/ncc-group-launches-soc-as-a-service-to-help-customers-experiencing-resource-shortages-and-office-closures-397977)
- Endpoint Detection and Response (https://newsroom.nccgroup.com/news/ncc-groups-instant-endpoint-detection-and-response-edr-solution-launched-to-detect-and-block-cyber-threats-targeting-remote-workforces-398237)
- NCSC has also produced some guidance on working from home securely and information on the criminal activity relating to COVID-19:
- NCSC Guidance for Staff (https://www.ncsc.gov.uk/guidance/home-working)
- Rise in criminal activity relating to COVID-19 (https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus)
- NCC Group has produced a cyber-threat intelligence report for the healthcare sector. The report has been shared with National CERTs, National Healthcare CERTs, or other organisations that serve as a national point of contact and that NCC Group communicates with about its COVID-19 healthcare initiative. Healthcare organisations are also sign up directly via our dedicated website: https://www.nccgroup.com/thankyouhospitals

References

1. https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/
2. https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/
3. https://www.computing.co.uk/news/4012969/hospitals- coronavirus-ransomware
4. https://www.zdnet.com/article/report-identifies-the-most-dangerous-mobile-app-store-on-the-internet/
5. https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware
6. https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/
7. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/would-you-exchange-your-security-for-a-gift-card/
8. https://blog.malwarebytes.com/threat-analysis/2020/03/apt36- jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
9. https://threatpost.com/coronavirus-apt-attack-malware/153697/
10. https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak
11. https://www.computing.co.uk/news/4012969/hospitals- coronavirus-ransomware
12. https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/
13. https://twitter.com/malwrhunterteam
14. https://www.virustotal.com/gui/file/9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967/details
15. https://www.cyber.gov.au/threats/advisory-2020-003-mailto-ransomware-incidents
16. https://www.dataprivacyandsecurityinsider.com/2020/03/covid-19-vaccine-test-lab-hit-by-maze-ransomware/
17. https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
18. https://research.nccgroup.com/2020/03/19/threat-actors-exploiting-the-pandemic/
19. https://www.bellingcat.com/news/2020/03/13/monitoring-and-debunking-covid-19-panic-the-haarlem-aldi-hoax/
20. https://www.forbes.com/sites/rachelsandler/2020/03/12/ny-attorney-general-orders-alex-jones-to-stop-peddling-fake-coronavirus-treatments/#454f87da8bbe
21. https://nationalpost.com/pmn/news-pmn/canada-news-pmn/military-says-no-link-between-military-vehicle-movement-and-covid-crisis-armed-forces
22. https://foreignpolicy.com/2020/03/30/beijing-coronavirus-response-see-what-sticks-propaganda-blame-ccp-xi-jinping/
23. https://www.independent.co.uk/news/uk/home-news/coroanvirus-origin-where-come-from-conspiracy-theory-chinese-lab-vodka-cocaine-garlic-a9436731.html
24. https://www.bbc.co.uk/news/blogs-trending-51271037

Image credits

Shutterstock: TippaPatt. Royalty-free stock photo ID: 583120876

Acknowledgements

Thanks to Luke Metcalf for his work on this advisory.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape. Through an unrivalled suite of services, we provide organisations with peace of mind that their most important assets are protected, available and operating as they should be at all times.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate and respond to the risks they face. We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

Headquartered in Manchester, UK, with over 35 offices across the world, NCC Group employs more than 2,000 people and is a trusted advisor to 15,000 clients worldwide.