CYJAX

Digital Intelligence
Securing the Future

COVID-19 Cyber Situation Report - 23 March 2020

CLIENT CONFIDENTIAL

TLP - GREEN

Purpose

This Cyber Situation Report is intended to help mitigate the risk of cyberattacks against public and private sector organisations during the coronavirus pandemic. It provides a broad overview of all coronavirus-related threats, alongside more general vulnerabilities that attackers could exploit. We at Cyjax hope this will help organisations and their staff protect themselves from cyber threats during this unprecedented crisis. All relevant IOCs are provided at the bottom of this report. If you require any further assistance or advice, please contact us.

Situation

Businesses, governments and their citizens around the world face an unprecedented challenge from the coronavirus pandemic. As of 23 March, there have been over 330,000 confirmed cases worldwide and 14,500 deaths. This includes 5,683 patients in the UK and 281 fatalities. [0] Strict restrictions have been placed on travel and freedom of movement as events are cancelled and borders closed. Shortages of food, medicines and essential supplies have all been reported as people panic buy and suppliers struggle to cope with increased demand. [1] In England, schools were shut for most pupils on 20 March and citizens instructed to practice social distancing. [2] On the same day, all pubs, restaurants, gyms and other social venues were ordered to close until further notice. Those that can work from home have been advised to do so while many others face redundancies or unpaid leave. Salaried employees forced to take temporary redundancies will receive up to 80% of their wages from the government. [3]

The economic damage is likely to be significant. The prices of oil, gold and other commodities are tanking. Investors fearing the impact on growth have withdrawn funds, wiping around a third off global markets since January. In the UK, interest rates have been cut to historic lows in a bid to temper the outbreak's economic impact. Exactly how effective this will be, remains to be seen. However, at 0.1%, there's very little room for further manoeuvre in monetary policy. [4] Airlines and holiday agents have borne the brunt of travel restrictions. As the EU bans travellers from outside the bloc for a period of 30 days, analysts estimate that up to 48,200 flights could be cancelled. Restaurant bookings have collapsed by up to 94% in some locations and the sale of cars has plummeted. [5]

Despite increasingly stringent measures being taken to slow the outbreak, both in UK hospitals and wider society, worst-case scenario forecasts suggest that up to 80% of the population could be infected. [6] At the time of publishing, this eventuality was looking increasingly likely as the British public failed to adhere to government guidelines on social distancing. On 21-22 March, thousands gathered in parks, markets and beaches around the UK, prompting the government to threaten more stringent measures if Britons refused to heed warnings. [7] Hospitals in the UK have been ordered to cancel all non-urgent operations for at least three months. Patients considered fit enough to leave will be sent home, and approximately 10,000 extra beds sourced from the private sector to ease pressure on NHS services. [8] Even the more positive estimates would severely strain NHS resources and result in thousands of deaths. It is difficult to accurately forecast the medium-long term impact of the pandemic. However, there is little doubt that COVID-19 is going to be massively disruptive for all sectors going forward.

Overview of malicious cyber activity

As the outbreak escalates, we are witnessing a significant uptick in cyberattacks exploiting the fear of coronavirus to compromise victims. Most sectors have been targeted, including government, manufacturing, pharmaceutical and

healthcare organisations. Employees working remotely for the first time have compounded the risk. In response, the National Cyber Security Centre (NCSC) provided guidelines for businesses and staff to work safely from home. [9]

Private citizens attempting to stay abreast of the latest developments have also been hit. Some have been infected with malware after visiting fake coronavirus tracking websites or mobile apps; others have received malicious emails impersonating the World Health Organization (WHO) or Centers for Disease Control and Prevention (CDC). A broad range of malware is being delivered via these vectors, including ransomware, remote access trojans (RATs) and information stealers (infostealers). Emails containing links to phishing pages are a persistent threat, including many purportedly offering coronavirus updates or advice. [10]

Fig.1 - Cyjax coronavirus-related incident reports

Offline criminals are also capitalising on the panic and confusion to defraud victims. Scammers have gone door-to-door impersonating NHS staff; some have offered to help quarantined people with their shopping for a small fee; others claim they are accepting donations to fund a vaccine. [11] Elsewhere, there have been reports of fake decontamination services being sold, as well as counterfeit coronavirus testing kits, medicines and protective equipment. [12] Large orders of face masks have been purchased that do not arrive and prices inflated for essential supplies, such as hand sanitiser and anti-microbial wipes.

Advanced persistent threat (APT) cyber activity

An Advanced Persistent Threat (APT) is a skilled offensive cyber group, usually backed or directed by a nation-state. In this section, we have also included details of any organised attack groups that present a significant threat to organisations. Most coronavirus-related APT activity up to this point has been observed in Asia. This is likely to reflect the fact that the outbreak began in China, providing cybersecurity researchers with more time to uncover and monitor campaigns in the region. This is not to say, however, that there has not been APT activity in other regions, merely that APTs in Asia are more likely to have been detected by this point.

Several malicious coronavirus-themed documents were identified that appear to have originated with North Korean APT @Kimsuky. [1, 2, 3] Some of these delivered BabyShark - a malware, favoured by the group, that is used to exfiltrate data from victims. It is not clear who these samples were targeting. However, previous @Kimsuky campaigns have attacked a broad range of organisations supporting Korean reunification, cryptocurrency exchanges, think tanks, nuclear power operators and more. [4]

Elsewhere in the region, Chinese APTs @MustangPanda, @ViciousPanda and @EmissaryPanda have been accused of using coronavirus-themed lures. [5, 6, 7] Various remote access tools have been delivered, including Cobalt Strike, PlugX RAT and the RoyalRoad dropper - used to download a custom RAT to exfiltrate information. These campaigns appear to have targeted Taiwan and the Mongolian public sector. However, all three groups are known to present a threat to organisations of interest to the Chinese state, including NGOs, foreign embassies, government, defence and technology sectors.

Russian cybercriminal group, @TA505, has been observed sending coronavirus-themed malspam to healthcare, manufacturing, and pharmaceutical organisations in the US. The emails have the subject "COVID-19 Everything you need to know" and contain a link to a ransomware downloader that can be used to further infect the machine. A separate @TA505 campaign targeting healthcare providers requests a Bitcoin payment to help develop "Remedies On Corona-Virus". [8]

As the coronavirus pandemic progresses, Business Email Compromise (BEC) will remain a significant threat to all sectors. In 2019, the FBI recorded 23,775 BEC incidents, resulting in more than $1.7bn in losses. [9] Already we have seen BEC gangs exploiting coronavirus to dupe victims. Cybercriminal group @AncientTortoise is believed to have been the first to employ this tactic. On 12 March, researchers captured an email from the group, claiming that their victim was changing bank accounts due to the spread of COVID-19. [10]

A DDoS attack against the US Department of Health and Human Services (HHS) website on 16 March 2020 was seemingly the work of a nation-state backed actor. Interestingly, it coincided with a disinformation campaign carried out via SMS, email and social media, claiming that a national quarantine of the US was imminent. While the DDoS attack did not cause any noticeable disruption to HHS operations, it may have been an attempt to disrupt the department's ability to dispel the rumours. Whether this was intended to undermine the government's response to COVID-19, or perhaps manipulate the US stock market, remains to be seen. [11]

Organised ransomware gangs will continue to present a significant threat to businesses. In the US alone last year, at least 966 government agencies, educational establishments and healthcare providers were infected, at a potential cost in excess of $7.5 billion. [12] The impact was often significant in ways other than just financial: operations were cancelled and patients sent to other hospitals; schools closed or lost students grades; essential local government services ground to a halt.

Interestingly, two of the most active ransomware groups operating at present, Maze and Doppelpaymer, have pledged to avoid targeting healthcare organisations during the coronavirus pandemic. This tactic is likely intended for self-preservation, rather than any genuine sense of altruism. Further, it still leaves numerous other operators, such as Sodinikobi/REvil, Ryuk, PwndLocker and Ako who have not made such claims. [13] Thankfully, several cybersecurity companies have offered free ransomware support services for healthcare providers. These include Emisoft and an alliance of firms working with C5 Capital.

Based on the available evidence, we assess it is highly likely that APTs will continue to exploit the COVID-19 pandemic to compromise targets. Consequently, it is essential that organisations maintain visibility on emerging APT campaigns targeting their sectors. Timely, accurate and actionable cyber threat intelligence is vital in this regard. Understanding a

group's tactics, techniques and procedures (TTPs) will allow an organisation to respond proactively, implementing effective mitigations that will minimise the likelihood of a successful breach.

Coronavirus-themed APT attacks

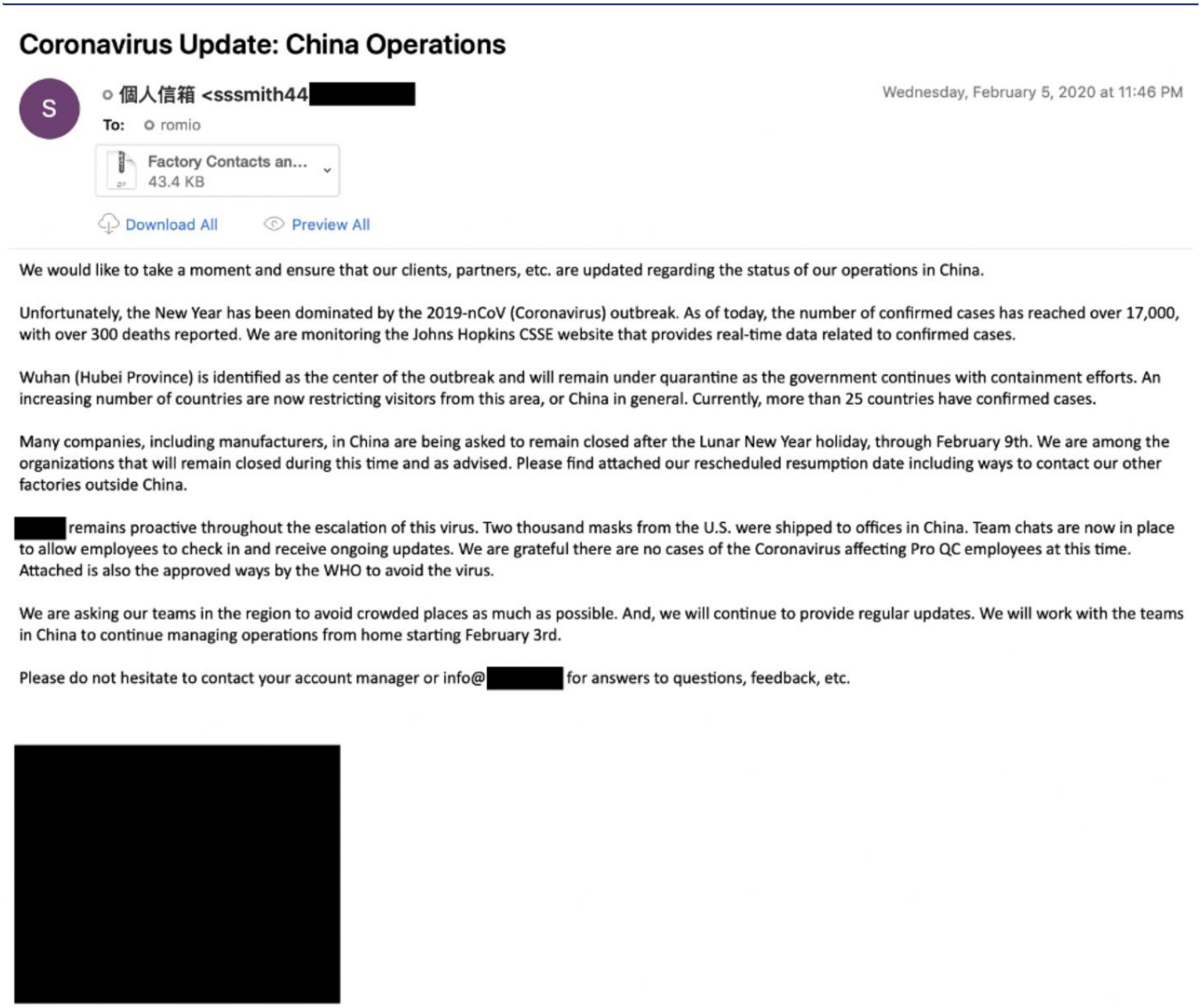
- North Korean APT Kimsuky was observed sending coronavirus-themed malicious documents to victims in the APAC region. [1]
- Chinese state-sponsored APT MustangPanda has distributed emails referencing coronavirus and Taiwanese deputy leader Chen Jianren. Malicious LNK files were attached that downloaded Cobalt Strike payloads. [2]
- Chinese APT ViciousPanda has reportedly been targeting Mongolian government departments with COVID-19-themed malicious RTF documents. These contained the RoyalRoad dropper, which downloads a custom RAT module to exfiltrate information. [3]
- Pakistani APT APT36 has been observed targeting the Indian government in a spear-phishing campaign. The lures, disguised as a coronavirus health advisory, delivered the Crimson RAT. [4]
- A coronavirus-themed malicious PDF has been discovered that pushes the PlugX RAT - linked to several Chinese APTs. In this instance, @EmissaryPanda (@APT27) was attributed. [6]

Malspam

There has been a significant uptick in malicious emails using coronavirus-themed lures to disseminate malware. A substantial number of these purport to have been sent from the World Health Organization (WHO) or Centers for Disease Control and Prevention (CDC). The types of lure documents and the strains of malware being used are wide-ranging. Victims have been sent malicious Word, Excel, ISO, PIF and PDF files, among others. These have delivered malware including the TrickBot banking Trojan, Ostap downloader, Remcos RAT, Emotet, Nanocore RAT, Agent Tesla keylogger, Lokibot infostealer, Ryuk ransomware, Hancitor Trojan and Bisonal malware. A feed of COVID-19 themed malware is available MalwareBazaar here.

In addition, researchers recently observed a notable new malspam campaign targeting the healthcare and manufacturing sectors in the US. The emails featured the subject "Please help us with Fighting corona-virus" and delivered the Redline Infostealer. This is a novel piece of malware offered as malware-as-a-service on Russian cybercrime forums. Subscriptions cost between $100 and $200 a month, depending on the package. The malware can steal login credentials, cookies, autocomplete fields and credit cards details, among other information. [1]

The variety of files and malware is indicative of the broad range of threat groups attempting to exploit the coronavirus pandemic. The lures will be refined over time depending on what is deemed to be most effective. Precedent suggests that the WHO, CDC and other major healthcare organisations will continue to be spoofed as people seek updated information on coronavirus. So far there has not been a significant number of fake NHS emails or documents reported. However, this is likely to change in the near future as the coronavirus response in the UK progresses. Details of 14 recent coronavirus-themed malspam campaigns are provided below.



Coronavirus Update: China Operations

S ○ 個人信箱 <sssmith44[redacted] Wednesday, February 5, 2020 at 11:46 PM

To: ○ romio

Factory Contacts an... 43.4 KB

Download All Preview All

We would like to take a moment and ensure that our clients, partners, etc. are updated regarding the status of our operations in China.

Unfortunately, the New Year has been dominated by the 2019-nCoV (Coronavirus) outbreak. As of today, the number of confirmed cases has reached over 17,000, with over 300 deaths reported. We are monitoring the Johns Hopkins CSSE website that provides real-time data related to confirmed cases.

Wuhan (Hubei Province) is identified as the center of the outbreak and will remain under quarantine as the government continues with containment efforts. An increasing number of countries are now restricting visitors from this area, or China in general. Currently, more than 25 countries have confirmed cases.

Many companies, including manufacturers, in China are being asked to remain closed after the Lunar New Year holiday, through February 9th. We are among the organizations that will remain closed during this time and as advised. Please find attached our rescheduled resumption date including ways to contact our other factories outside China.

[redacted] remains proactive throughout the escalation of this virus. Two thousand masks from the U.S. were shipped to offices in China. Team chats are now in place to allow employees to check in and receive ongoing updates. We are grateful there are no cases of the Coronavirus affecting Pro QC employees at this time. Attached is also the approved ways by the WHO to avoid the virus.

We are asking our teams in the region to avoid crowded places as much as possible. And, we will continue to provide regular updates. We will work with the teams in China to continue managing operations from home starting February 3rd.

Please do not hesitate to contact your account manager or info@[redacted] for answers to questions, feedback, etc.

[redacted]

Fig 2. Example of coronavirus-themed malspam

Coronavirus-themed Malspam

- Italian users are being targeted with emails purporting to be from Dr Penelope Marchetti of the World Health Organisation (WHO). The emails contain a malicious Word document that delivers the TrickBot banking Trojan and Ostap downloader. [1]
- Emails impersonating the Centers for Disease Control and Prevention (CDC) are being sent with the subject: "Re: nCoV: Coronavirus outbreak and safety measures in your city (Urgent)". A malicious ISO file delivers the Remcos RAT. [2]
- Japanese targets have been sent emails warning of coronavirus infections in local prefectures. A malicious Word document is attached that delivers the Emotet payload. [3]
- Emails with the subject "Coronavirus Update: China Operations" are being distributed with a compressed PIF file attached. When run, the document downloads and installs the Nanocore RAT. [4]
- Spoofed WHO emails have been distributed with the subject "Attention: List Of Companies Affected With Coronavirus March 02, 2020". A malicious Excel document is attached that delivers the Agent Tesla keylogger. [5]

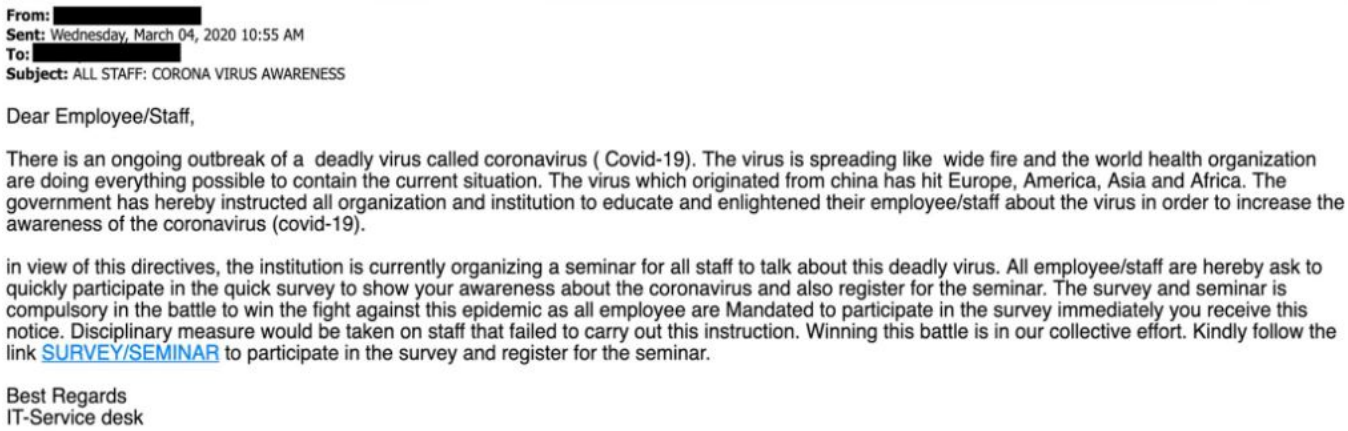
- Attackers impersonating the Ukrainian Ministry of Health distributed an email purportedly containing the latest news on COVID-19. It delivered a backdoor written in C#. [6]
- Threat actors impersonated FedEx to deliver an email with the subject "Coronavirus Customer Advisory Issue". A malicious executable disguised as a PDF document was attached. Once opened, users are infected with the Lokibot infostealer. [7]
- Thai targets were sent emails claiming to be from the Ministry of Public Health and the National Institute of Health of Thailand. The emails featured the subject, "Fwd: Re: CoronaVirus Express Information" and delivered the Nanocore RAT. [8]
- The Hancitor Trojan is being distributed in emails purporting to be from insurance company Cigna. These are masquerading as an invoice for a coronavirus insurance plan. [9]
- Coronavirus-themed documents claiming to be sent from the Ministry of Social Affairs of the Republic of Estonia are delivering a generic keylogger. [10]
- A variant of the Ryuk ransomware was discovered that references a new case of coronavirus in Hong Kong. [11]
- The Bisonal malware is being distributed in emails that reference the Church of Shincheonji, believed to be the epicentre of the coronavirus outbreak in South Korea. [12]
- Threat actors have been delivering the RoyalRoad dropper in malicious RTF documents. These reference the financial budget for Kyrgyzstan amid the coronavirus. When the macros are run, the Chinoxy keylogger is downloaded and executed. [13]
- Malspam claiming to be from Dr Stella Chungong at the WHO is distributing the Netwire RAT. [14]

Malicious Websites

There has been a significant increase in suspicious coronavirus-themed domains registered in the past few months. Since January 2020, more than 4,000 coronavirus-related domains have been registered globally. Approximately 3% of these were confirmed as malicious and an additional 5% deemed suspicious. Based on these figures, coronavirus-themed domains are approximately 50% more likely to be malicious than others registered during the same period. [1] A feed of suspicious new COVID-19 domains, courtesy of security researcher 'dustyfresh', is available here.

Some of these domains have hosted websites masquerading as coronavirus tracking maps. A notable example imitated the John Hopkins University Coronavirus Map, which is tracking cases worldwide. When users visited the fake site, they were infected with the Azorult infostealer. [2] Similar pages have also distributed the DanaBot banking trojan. [3] In one instance, a fake "Public Health Agency of Canada" website distributed a malicious Word document that dropped the Ursnif (Gozi) banking Trojan [4]. All of these malware are designed to capture sensitive victim information, including logins for banks, email accounts and social media platforms.

Standard phishing pages are also being delivered in coronavirus-themed emails. In many instances, these are untargeted and distributed in bulk to potential victims. However, there have also been instances of targeted coronavirus phishing campaigns. A notable example was received by NHS personnel. The emails appeared to have been sent from an internal IT department and featured the subject "ALL STAFF: CORONA VIRUS AWARENESS". Contained within the body was a link to an Outlook Web App phishing page. [5]



From: [redacted]
Sent: Wednesday, March 04, 2020 10:55 AM
To: [redacted]
Subject: ALL STAFF: CORONA VIRUS AWARENESS

Dear Employee/Staff,

There is an ongoing outbreak of a deadly virus called coronavirus (Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit Europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link SURVEY/SEMINAR to participate in the survey and register for the seminar.

Best Regards
IT-Service desk

Fig 3. Phishing email sent to NHS personnel

Given the evidence so far, we expect the creation of coronavirus-themed domains to escalate in the near term. Many of these will impersonate national and supranational health bodies, including the WHO, CDC and NHS. Others will purport to offer updates about the virus, its spread and a potential cure. Most will be benign; however, approximately 5% will be malicious, hosting scams, harvesting credentials, or delivering malware, including ransomware, banking Trojans and infostealers. Consequently, all non-official coronavirus-themed domains should be treated with suspicion and avoided where possible.

Staff across all sectors are highly likely to continue receiving both targeted and generic coronavirus-themed phishing emails going forward. Many of these will likely appear to have been sent from the UK government, CDC or WHO. Indiscriminate campaigns will probably link to generic phishing pages for Microsoft services, social media platforms and online banking. Targeted attacks could feature a link to a specially crafted phishing page, designed to look like an official company login portal. Entering credentials into these pages could put the entire organisation's internal network at risk of compromise. As always, using unique, complex passwords and employing robust multi-factor authentication will significantly reduce the likelihood of a successful breach.

Coronavirus-themed malicious websites

- Phishing emails with the subject "Re:SAFTY CORONA VIRUS AWARENESS WHO" are spoofing Dr Stella Chungong from the WHO. The emails link to a fake WHO website that harvests user credentials. [1]
- Security researcher JcyberSec_discovered two Coronavirus-themed phishing pages that had been sent to Huawei personnel. When accessed, a pop-up requested that users verify their email address and password. Both sites are now offline. [2]
- Emails impersonating the CDC with the subject "COVID-19 – Now Airborne, Increased Community Transmission" have been distributing Outlook phishing pages. The display name is spoofed as "CDC INFO" and appear to have been received from CDC-Covid19@cdc.gov. [3]
- A new strain of ransomware, seemingly linked to the Kbot infostealer, is being distributed via fake websites advertising WiseCleaner software. The ransom note references coronavirus and renames the drive to "CoronaVirus". [4]
- Threat actors have spoofed the CDC Health Alert Network to send emails seemingly containing a link to updated coronavirus infection figures. In reality, the victim is redirected to an Outlook-themed phishing page. [5]

Malicious Apps

As the pandemic has progressed, developers have begun disseminating malicious coronavirus-themed Android apps on Google Play and unofficial app stores. At the time of publishing, far fewer apps had been discovered than malicious domains, reflecting the time and effort that it takes to develop an app compared to creating a malicious website or launching a phishing campaign. Security researcher, Lukas Stefanko, is maintaining a list of new coronavirus-themed Android malware, available here.

The apps are similar in tactics and appearance, luring victims hoping to learn how to cure coronavirus, track its spread, or identify at-risk groups. Several variants are delivering the Cerberus Android banking Trojan, a remote access malware with the ability to conduct overlay attacks, gain SMS control, bypass two-factor authentication (2FA) and harvest the victim's contact list. [1] Another notable example disguised as a Coronavirus Tracker app is distributing a new Android ransomware, dubbed CovidLock. The threat actors threaten to wipe the phone and leak the victim's social media accounts unless the victim pays $100 in Bitcoin within 48 hours. [2] Researchers recently discovered a master password to unlock devices infected with CovidLock - 4865083501. [3]

Over time, malicious coronavirus-themed apps are expected to proliferate. These are likely to become increasingly sophisticated, as cybercriminals invest time and money creating more convincing and effective apps. Victims face the risk of financial costs, identity theft and data loss. Healthcare organisations, by contrast, may find it more difficult to disseminate potentially life-saving information, if users become wary of trusting apps and websites distributing coronavirus updates. To mitigate this risk, users should avoid downloading apps from unofficial sources. Third-party Android app stores present the greatest risk. However, malware is still prevalent on the Google Play Store and, to a much lesser degree, the Apple App Store. If in doubt: do not download.

Coronavirus-themed apps

- Google removed AC19, a coronavirus infection tracking app developed by the Iranian government, from the Play store. Once installed, the app could harvest information such as phone numbers, contact lists and location data. [1]
- Vodafone 5G customers were targeted with Cerberus from a malicious coronavirus-tracking-app website. [2]

Fraud

As expected, cybercriminals distributing malware and harvesting credentials are not the only ones hoping to profit from the pandemic. Scammers are also increasingly exploiting fear of coronavirus to defraud victims. Since 9 February, Action Fraud has received 105 reports of coronavirus-related-fraud, resulting in collective losses of nearly £970,000. In March alone, reports of coronavirus-related fraud increased 400%. Most of these involved online shopping scams where people have ordered face masks, hand sanitiser and other items which never arrived. Others have impersonated the CDC and WHO, requesting funds in Bitcoin to access essential information. Investment scams, advising people to profit from the coronavirus downturn, have also been reported. [1]

Instances of offline fraudsters impersonating NHS staff have also been uncovered. Towns and cities across the UK have reported door-to-door scammers offering to help with shopping for payment or collecting donations to fund a vaccine. [2] The sale of fake coronavirus testing kits is also a concern. Some of these have contained purified water vials valued at nearly $200. [3] Even fake vaccines are being sold. On 22 March, the US Justice Department issued a restraining order against a website offering WHO vaccine kits for $4.95. [4] For victims, such scams present a risk of

financial loss, coupled with the potential of providing a false sense of security. If an infected person uses a fake coronavirus vaccine or testing it, they may not seek essential medical treatment and inadvertently spread the disease to others.

Shortages of essential products such as hand sanitiser and anti-microbial wipes have also been reported in many places. Predominantly, this reflects the unprecedented demand generated by the coronavirus outbreak. However, it has also been exacerbated by 'price gougers' purchasing large stocks to sell at a profit. Online retailers like Amazon and eBay have clamped down on this practice but shortages of essential products remain in some places. [5] Thankfully, many distilleries have begun producing hand sanitiser alongside their usual products, helping to bolster supplies. [6]

As expected, the unprecedented demand for protective equipment has fuelled a burgeoning supply of counterfeit goods. During a week of action, Interpol seized more than 34,000 counterfeit and substandard masks, alongside various fake products, including "corona spray", "coronavirus packages" and "coronavirus medicine". [7] Many of these are now being offered for sale on the darknet, as can be seen below. Some will be genuine products, potentially purchased by price gougers before the restrictions on sale were implemented. Others will undoubtedly be fake, putting the purchaser's health at risk alongside those that they come into contact with.

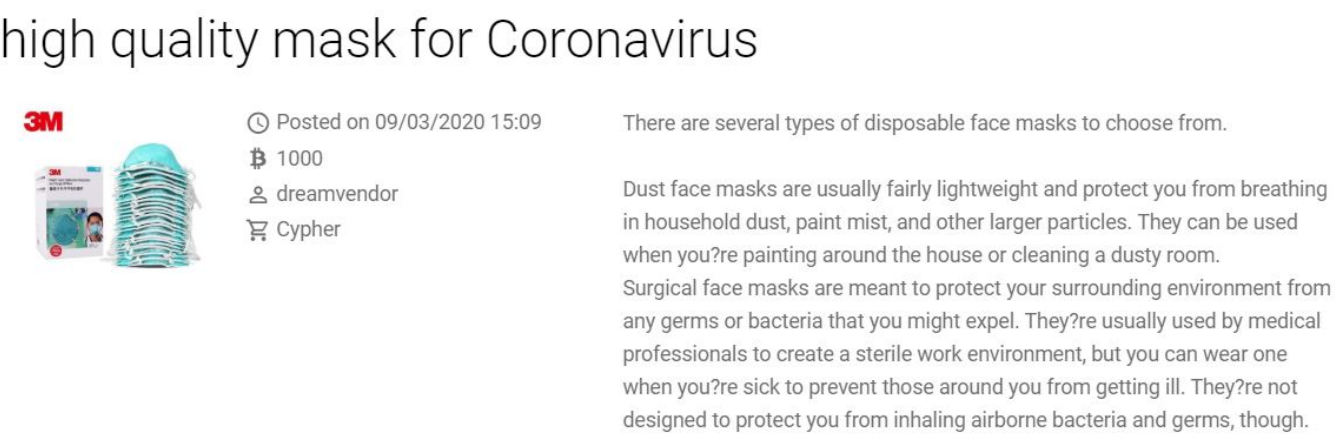


Fig 5. Face masks advertised for sale on the Cypher darknet market

Offline coronavirus fraud

- In France, men dressed as police have demanded Chinese students pay fines for wearing masks, which allegedly contravened the country's laws against full-face veils. [1]
- The Canadian Anti-Fraud Centre has warned that fraudsters are going door-to-door and offering fake decontamination services. [2]

Advice

- Ensure antivirus software is kept up to date.
- Do not open files or links from sources that you do not know.
- Be suspicious of any vendor requesting to divert payments to a different bank account. Always verify that the switch is legitimate.
- Avoid coronavirus-themed apps and unofficial websites.
- Test staff with coronavirus-themed phishing simulations.
- Delete emails claiming to be from the CDC or WHO. The latest updates from both are available here and here.

- Ignore all online adverts for vaccinations.
- Only purchase masks, hand sanitiser and related products from reputable stores.

Indicators of Compromise (IOCs)

- 7818bab9eef0d0ad71b094ad2baacfbb
- e76c84b3e25207cce5cdd85261692626
- 0deb9ee326eb1bcf7b615c543ac28f3c
- 0c3239fdda3c9517c0d8437875d25eb9
- e76c84b3e25207cce5cdd85261692626
- fc00964131a8c9407ba77484e724fc9d
- 6a3b792208bd433a2ceff4f8321561a0
- bc466506e3f184c45054c93445275d9b8ef044f8
- 54afa3a4e2ca8ac91c4f54641e267c78d58948b9
- afabf51065d63ea7edc95af3c8548ad774321202
- f224fc2f1a2ce1e3e1d1ff9d194405e99157725e
- CBB32307586F83D070BB84AD6C26DD73
- c844992d3f4eecb5369533ff96d7de6a05b19fe5f5809ceb1546a3f801654890
- b41e2237590421056f41a33b004670abf29dc83157b1f38c0eab65ecfd6b9663
- 6b61c223d618ead7ca78f4731a0128e30bf602bdfe8d940e442041486cb2fe76
- 58e918466a61740abe42a2d1ca29bd8d56daf53912e6d65879cbe944466fb80c
- 8e3240a2a6b07ae8a6fde884c0e18e476ca3e92438022fe1a1ad4b2ba2334737
- 345d8b4c0479d97440926471c2a8bed43162a3d75be12422c1c410f5ec90acd9
- dd7023dd82b641c9307566b87acf0951f16b27c34094a341fa1fe7671d269bf4
- 9aea43b22f214228caf4fc714f426c0a140b7dd70b010bf3778cd1c0ec440851
- 906EFF4AC2F5244A59CC5E318469F2894F8CED406F1E0E48E964F90D1FF9FD88
- ee8a404264b4d3144bc37ef7118da24c77dd15b20d38250badbf53140f7c1d2a
- e82d49c11057f5c222a440f05daf9a53e860455dc01b141e072de525c2c74fb3
- 4f6d4d8f279c03f1ddfa20f95af152109b7578a2bec0a16a56ff87745585169a
- 6897a3b85046ba97fb3868dfb82338e5ed098136720a6cf73625e784fc1e1e51
- 8a9333204db83c2571463278cb6a6241ae5f215b2166bf4af5693d611049d5a9
- 8da0eb3a2378d218043e9f3188e59e3158f1fd01bbcd979f05197c74c2fb7a1c
- 291a4eb06358eca87fbc1f133ee162b6c532f4ec3e6f39c2646cde5de60e80f9
- 5987a6e42c3412086b7c9067dc25f1aaa659b2b123581899e9df92cb7907a3ed
- a08db3b44c713a96fe07e0bfc440ca9cf2e3d152a5d13a70d6102c15004c4240
- 3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3
- 6117a9636e2983fb087c9c9eec2a3d2fbadb344a931e804b2c459a42db6d2a68
- e02aedeea6c8dc50a5ff95d37210690daeeef172b2245e12fcf0913a492fd0ac
- 0ddd7d646dfb1a2220c5b3827c8190f7ab8d7398bbc2c612a34846a0d38fb32b
- 5df956f08d6ad0559efcdb7b7a59b2f3b95dee9e2aa6b76602c46e2aba855eff
- 876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656
- 20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a
- 0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010
- b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748
- 2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
- 0b3e7faa3ad28853bb2b2ef188b310a67663a96544076cd71c32ac088f9af74d

- 13c0165703482dd521e1c1185838a6a12ed5e980e7951a130444cf2feed1102e
- Fda64c0ac9be3d10c28035d12ac0f63d85bb0733e78fe634a51474c83d0a0df8
- 126569286f8a4caeeaba372c0bdba93a9b0639beaad9c250b8223f8ecc1e8040
- 203c7e843936469ecf0f5dec989d690b0c770f803e46062ad0a9885a1105a2b8
- 2a469268fb18f0b009dc5b2bdd47f9ed61f0a3a2de04ba39daccd08a13fb19b2
- 95489af84596a21b6fcca078ed10746a32e974a84d0daed28cc56e77c38cc5a8
- f74199f59533fbbe57f0b2aae45c837b3ed5e4f5184e74c02e06c12c6535f0f9
- 9d52d8f10673518cb9f19153ddbe362acc7ca885974a217a52d1ee8257f22cfc
- 7f230a023a399b39fa1994c3eaa0027d6105769fffaf72918adebf584edc6fe0
- 604679789c46a01aa320eb1390da98b92721b7144e57ef63853c3c8f6d7ea85d
- a49133ed68bebb66412d3eb5d2b84ee71c393627906f574a29247d8699f1f38e
- c360e6b8ac7e915d745b4c2c80cd56c452b666be55a5a639e59b0091ce531a6c
- de1b53282ea75d2d3ec517da813e70bb56362ffb27e4862379903c38a346384d
- 8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160
- 9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967
- 238a1d2be44b684f5fe848081ba4c3e6ff821917
- 69a6b43b5f63030938c578eec05993eb
- a4388c4d0588cd3d8a607594347663e0
- 1b6d8837c21093e4b1c92d5d98a40ed4
- 4008eec5413e2cf20bb1d6d039d027fdab6e0283
- bda2e2ba4e4deb14b27fb6e52f255dfebf7bdbfa
- 599db33d534d1e98ea63dd2ce30100a7
- 05adf4a08f16776ee0b1c271713a7880
- ef07feae7c00a550f97ed4824862c459
- FDB2F4EFA95DD8B5EAD7527C92F24542
- 4202C9E8835552CD64F6A978FDF6BAAB
- 45.128.134[.]14
- 23.19.227[.]235
- 123.51.185[.]75
- 95.179.242[.]6
- 95.179.242[.]27
- 199.247.25[.]102
- 95.179.210[.]61
- 95.179.156[.]97
- 110.236.210.87
- 202.195.34[.]6
- 217.182.56[.]71
- 218.2.138[.]4
- 167.214.156[.]174
- 66.206.18[.]186
- 107.175.64[.]209
- 64.188.25[.]205
- hxxps://hausbauen24.net/wp-content/who/who/COVID-19/?trk=Wuhan202001&Verify=ODk3NmRmaDg5N2doQGRmZzg3LmNvbQ==
- hxxps://jayalbertandassociates.com/sector/who/COVID-19/?trk=Wuhan202001&Verify=c2hhb0BodWF3ZWkuY29t

- hxxps://185 234.73.125/wMB03o/Wx9u79.php
- punditx.duckdns[.]org:9993
- octocrypt.duckdns[.]org:9993
- hxxp://healing-yui223[.]com/cd[.]php
- hxxp://skakkiopiskattkio[.]info
- hxxp://crphone.mireene[.]com
- hxxps://www[.]schooluniformtrading[.]com[.]au/cdcgov/files/
- hxxps://drive.google[.]com/uc?export=download&id=1vljQdfYJV76IqjLYwk74NUvaJpYBamtE
- hxxp://covid19-guidelines[.]online/UpdateFlashPlayer_11_5_2[.]apk
- hxxps://onthefx[.]com/cd[.]php
- hxxps://urbanandruraldesign[.]com[.]au/cdcgov/files
- hxxps://gocycle[.]com[.]au/cdcgov/files/
- hxxp://euromed.com[.]ua/cmgtkz/cgcjp.php
- hxxp://shorelinezero[.]com/fiHRD
- hxxp://tbdtech.com.vn/modules/sanny[.]php
- hxxp://team-galena.com/checks/woodmarine[.]php
- hxxp://tedxggdsdcollege.in/xwzp/suziemulhall[.]php
- hxxp://terdance.ru/wp-includes/weaverja2000[.]php
- hxxp://teresaoefinger.com/u2l/yngwll57[.]php
- hxxp://testtesttest.cloud/language/wschramm2001[.]php
- hxxp://coronasafetymask[.]tk
- hxxp://coronavirusapp[.]site
- hxxp://thanhxuanvietcom/ktzoq9aicz/williamwoo1668[.]php
- hxxps://bitbucket[.]org/example123321/download/downloads/foldingathomeapp.exe
- hxxp://theazsmiths.com/name/rjanzikcom[.]php
- hxxp://thechristianmind.org/.well-known/ykasan[.]php
- hxxp://thehousejumpers.com/ffr/willhayn[.]php
- hxxp://imbc.onthewifi.com/ks8d [IP address] akspbu[.]txt
- hxxps://coronaviruscovid19-information[.]com/en/
- hxxps://coronaviruscovid19-information[.]com/tr/
- hxxps://corona-virus-map[.]net/map.jar
- hxxps://corona-map-data[.]com/bin/regsrtjser346.exe
- hxxps://corona-virus-map[.]net/map1.jnlp
- hxxps://coronavirus-apps[.]com
- dw.adyboh[.]com
- wy.adyboh[.]com
- feb.kkooppt[.]com
- compdate.my03[.]com
- jocoly.esvnpe[.]com
- bmy.hqoohoa[.]com
- bur.vueleslie[.]com
- wind.windmilldrops[.]com
- coronavirusapp[.]site
- dating4sex[.]us
- dating4free[.]us
- perfectdating[.]us

- redditdating[.]us
- email.gov.in.maildrive[.]email/?att=1579160420
- email.gov.in.maildrive[.]email/?att=1581914657
- Postmaster[@]mallinckrodt[.]xyz
- brentpaul403[@]yandex[.]ru
- phc859mgge638@inbox[.]ru

STATEMENT OF CONFIDENTIALITY

This document contains confidential trade secrets and proprietary information of Cyjax Limited. The recipient is expected to treat this document as they would their own confidential internal material. Neither this document, nor any diagrams contained in this document, may be disclosed to any person outside of the recipient's organisation without express written permission from Cyjax Limited. By accepting this document, the recipient affirms that they will comply with these expectations.

Cyjax Limited, Registered in England and Wales no 08302026.
Registered Office 8th Floor, 6 Mitre Passage, London SE10 0ER.
United Kingdom.

CYJAX
Cyjax Limited
6 Mitre Passage
Greenwich
London SE10 0ER
info@cyjax.com
+44 (0)20 7096 0668
CYJAX.COM