CYJAX

Digital Intelligence
Securing the Future

# COVID-19 Cyber Situation Report - 31 March 2020

CLIENT CONFIDENTIAL

TLP - GREEN

**Updated edition - original 23 March 2020**

## 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 face an unprecedented challenge from the coronavirus pandemic. As of 31 March, there have been over 765,081 confirmed cases worldwide and 36,868 deaths. This includes 22,141 patients in the UK and 1,408 fatalities. [1] 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. [2] In the UK, all non-essential businesses have been closed, including pubs, restaurants, gyms and other social venues. People have been ordered to stay in their homes except for "very limited purposes". [3] Those that can work from home are doing so; many others have been made redundant and are now surviving on state benefits. [4]

The economic damage is likely to be significant. The prices of oil, gold and other commodities have plummeted. Investors fearing the impact on growth have withdrawn funds, wiping around a third off global markets since January.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. [5] Airlines and holiday agents have borne the brunt of travel restrictions. Thousands of flights have been cancelled, stranding up to a million Britons abroad. On 30 March, the government announced it would be committing £75m to help repatriate those that couldn't secure a flight home. [6]

Despite increasingly stringent measures being taken to slow the outbreak, both in UK hospitals and wider society, the number of cases continues to grow. Hospitals in the UK have cancelled all non-urgent operations for at least three months. Patients considered fit enough to leave have been sent home, and approximately 10,000 extra beds sourced from the private sector to ease pressure on NHS services. [7] Despite these measures, NHS resources are under severe strain and thousands more deaths are anticipated. It is difficult to accurately forecast the medium to long term impact of the pandemic. However, there is little doubt that COVID-19 is going to be massively disruptive for all sectors for the foreseeable future.

## 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, pharmaceuticals 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. [8]

Private citizens attempting to stay informed 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, advice or investment opportunities. [9]

Even those wishing to simply stay in touch with friends and colleagues are not safe. Users of Zoom (for both business and personal calls) are at risk from a large spike in fake domains. An estimated 1,700 new domain names containing the word “Zoom” have been created since January. Fake sites impersonating genuine Zoom domains are the most common, with threat actors attempting to capture users’ personal details; other fake sites push other apps alongside the free software, such as InstallCore. [10]

Recreational callers are not immune: the popular House Party video chat app, which rose to number one on the App Store in the third week of March, appears to have been compromised. Users looking to delete the app have been asked for their password to 'complete deactivation'; following this, suspicious logins from unrecognised IP addresses or devices on Instagram, Twitter, Spotify, and Netflix have been seen. Subsequent research suggests that in, fact, some users may have reused credentials, entered the login information at a different malicious site, or installed a malicious app. House Party has stated that “All Houseparty accounts are safe - the service is secure, has never been compromised, and doesn’t collect passwords for other sites.” [11, 12, 13]

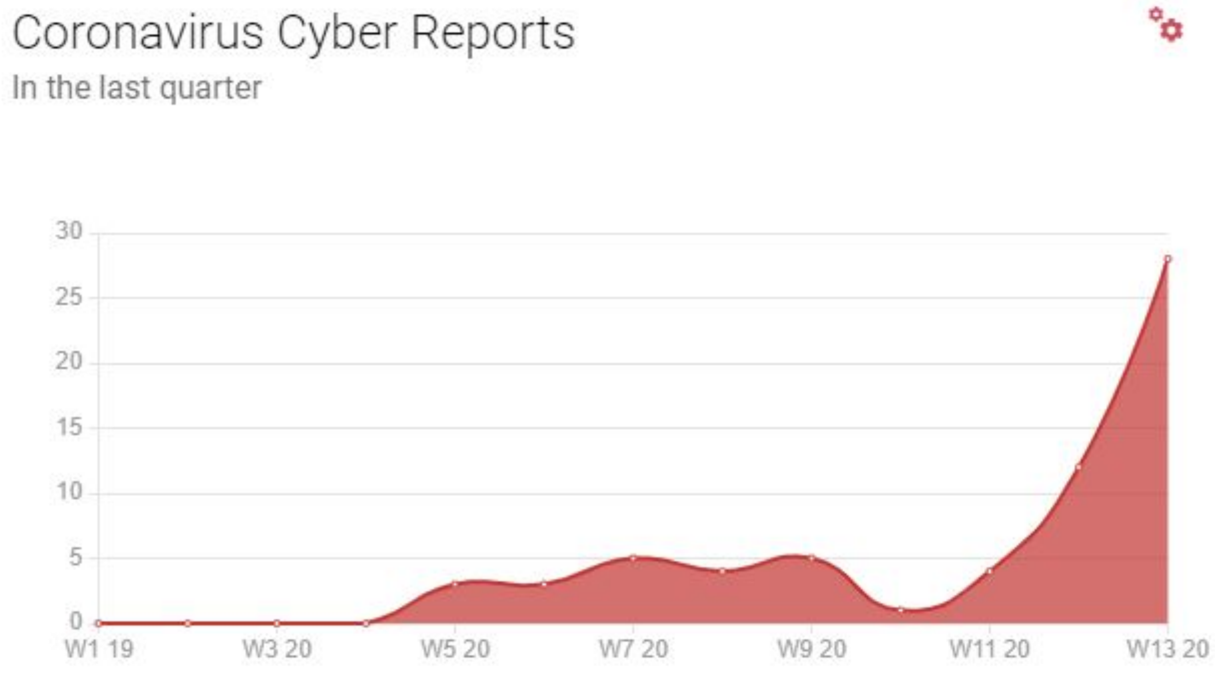


**Fig.1 - Cyjax coronavirus-related incident reports**

Disinformation, misinformation and conspiracy theories are rife. The situation has become so serious that the World Health Organization (WHO) declared an "infodemic" and warned of the potential impact on global health. [14] Unsubstantiated claims about the origin and scale of the disease, its prevention and treatment, have circulated on social media, via text messages, and in Russian and Chinese state media. Some claim that the Chinese were either deliberately or inadvertently responsible; others allege that the disease is a US bio-weapon. According to the EU, Russian media sources have promulgated the latter narrative in a bid to stoke "confusion, panic and fear". Allegedly, this is part of a broader strategy to "subvert European societies from within". [15]

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. [16] Elsewhere, there have been reports of fake decontamination services being sold, as well as counterfeit coronavirus testing kits, medicines and protective equipment. [17] 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 Word 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. Targets included South Korean think tanks, government organisations, news corporations, and university professors, among others. Previous @Kimsuky campaigns have focused on a similarly broad range of targets, including 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 deceive 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]

The World Health Organization (WHO) has also been targeted. On 13 March, an unidentified APT activated a malicious site that was mimicking the WHO's internal email system. The attack was unsuccessful but researchers noted that the same infrastructure had also been used to target other healthcare and humanitarian organisations in recent weeks. [12 ] Some have speculated that @DarkHotel may have been responsible. The suspected North Korean APT group has engaged in cyberespionage operations against a broad range of targets since at least 2007.

Organised ransomware gangs will continue to present a significant threat to businesses. In the US last year, at least 966 government agencies, educational establishments and healthcare providers were infected, at a potential cost in excess of $7.5 billion. [13] 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. [14] This was demonstrated to be the case, as overnight on 26 March the security researcher observed Ryuk being deployed against an unnamed US healthcare provider. 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 organisations 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]
- UK-based Hammersmith Medicines Research was infected with Maze ransomware, despite the group's pledge to spare the healthcare sector during the coronavirus pandemic. Fortunately, the company was able to repel the attack and quickly restore all functions. [7]

## Cyjax

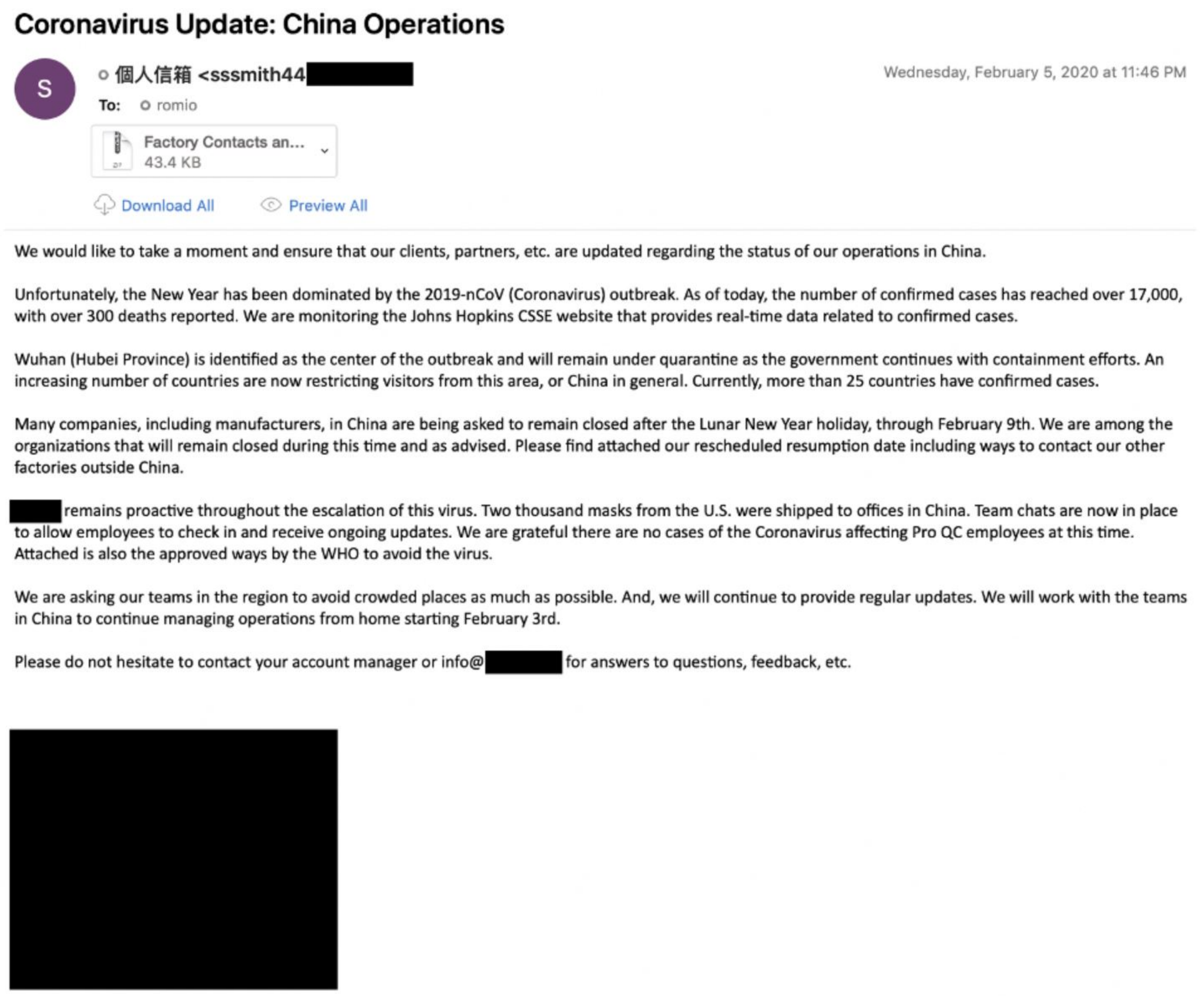
- The Ryuk ransomware attackers are continuing to target hospitals, despite the ongoing pandemic. Ryuk is traditionally delivered by TrickBot. Consequently, any organisation infected with the Trojan should initiate incident response proceedings immediately. [8]

## 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 via 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 19 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

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]

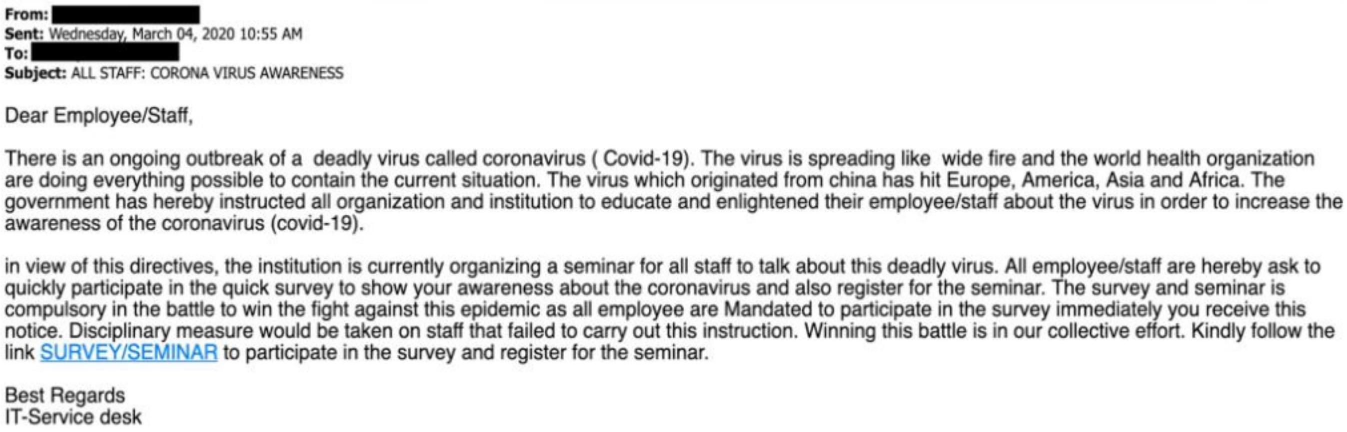
- Attackers impersonating the Ukrainian Ministry of Health distributed an email purportedly containing the latest news on COVID-19. It delivered a backdoor written in C#. [6]
- Threat actors impersonated FedEx to deliver an email with the subject "Coronavirus Customer Advisory Issue". A malicious executable 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]
- Emails purporting to come from the victim's insurance provider have been distributing a Microsoft Office 365 phishing page. Another uses a fake DocuSign lure, which purports to contain details about whether COVID-19 testing is covered under the company's health insurance plan. [15]
- The WarZone RAT is being delivered in COVID-19 themed phishing emails. The attackers issue health warnings purportedly from the CDC that contain advice attached in malicious Word Documents. If opened, CVE-2017-11882 (Microsoft Office bug) is exploited and the RAT is downloaded and installed. [16]
- The NetWalker ransomware is being delivered in phishing lures, targeting Spanish hospitals. The emails purport to offer "information on COVID-19", but with PDF attachments that activate the ransomware, commonly associated with computer crime groups in Eastern Europe. [17]
- A coronavirus-related phishing campaign has been observed imitating a local hospital in Canada. The email tells the recipient that they have been exposed to coronavirus through a colleague, friend, or family member, and need to be tested. Malicious macros in the document are used to install malware which steals cryptocurrency wallets, browser cookies, and device information, as well as looking for open shares on the network. [18]
- The Zeus Sphinx Trojan (AKA Zloader, Terdot) has returned after nearly three years of activity and is now being pushed in coronavirus-themed malspam. [19]

## 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, published by 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 CDC and NHS, and the WHO. Others will offer purported 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.

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.

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 an 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]
- A scam site was discovered advertising "Corona Anti-Virus", which claims to protect the user from COVID-19 while the software is running. Installing the app infects the user with the BlackNET botnet - a piece of malware that can deploy DDoS attacks, take screenshots, steal passwords and Bitcoin wallets, implement a keylogger, execute scripts and more. [6]
- A watering hole campaign is targeting iOS users in Hong Kong. It is distributing a new mobile malware, dubbed lightSpy, via local news links. The topics used as lures were either sex-related, clickbait, or news related to the COVID-19 disease. Information collected by lightSpy includes connected WiFi history, contacts, GPS location, hardware information, iOS keychain, call history, browser history, SMS messages, available WiFi network, local network IP addresses, Telegram, QQ, and WeChat credentials. [7]
- An HHS.gov (US Department of Health & Human Services) open redirect is being used by threat actors to spread the Raccoon infostealer to US targets, using coronavirus themes emails as a lure. [8]
- A new attack is hijacking D-Link and Linksys routers' DNS settings. Web browsers display alerts for a fake COVID-19 information app from the WHO which actually delivers the Oski infostealer. [9]
- The operators of the Ginp banking Trojan have created a web page called "Coronavirus Finder", which shows the number of people infected with the coronavirus near the user. Visitors to the site are asked to pay a small fee to see the coronavirus victim's location but information entered into the payment page is stolen. [10]
- Threat actors running the WordPress WP-VCD malware have begun to distribute pirated coronavirus-themed plugins that inject a backdoor into websites. These appear as legitimate plugins, named "COVID-19 Coronavirus - Live Map WordPress Plugin", "Coronavirus Spread Prediction Graphs", and "Covid-19". [11]
- UK government phishing sites have been modified to offer the promise of COVID-19 aid or relief. Others are distributing malware, including the DanaBot banking Trojan. [12]

## 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 deliver 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]
- Additional coronavirus-themed domains have been discovered distributing Cerberus in fake apps: ‘Covid-19-tracker.apk’ and ‘Corona-Apps.apk’. [3]
- Malicious websites that offer "ways to get rid of the Coronavirus" have been distributing the Anubis Android banking Trojan. The files sites host malicious APK files entitled "Covid-19.apk" or “Corona.apk”, which are used to infect victims. [4]
- A malicious version of a legitimate COVID-19 app by SoftMining is targeting users in Italy. Threat actors downloaded the legitimate SoftMining app, injected malicious code into it, and then recirculated it to targets. Once installed, it can collect a victim’s camera, GPS location, microphone, contacts, calls, texts, and storage. [5]
- A new variant of the Ginp mobile banking Trojan is leveraging the coronavirus to steal payment data. Users in Spain appear to make up the majority of the victims. Ginp opens a web-page called 'Coronavirus Finder': the page has a simple interface showing the number of people infected with the coronavirus near the visitor, urging them to pay a small sum to see the exact location of the infected. That money is sent to the attackers and the payment data is skimmed. [6]
- The Saudi Arabian Health Council is being impersonated in a watering hole attack that delivers the AdoBot Android spyware. AdoBot’s features include real-time command execution, schedule commands, hidden app icons, fetch calls, SMS, and contacts, monitor GPS location, update APK remotely. [7]
- Another Anubis distribution method has been identified that lures victims with an “8GB gift to all who fight against COVID-19!”. However, to get the free 8GB, recipients must download an APK that installs the Anubis banking Trojan. [8]
- A new mobile malware - Android Xerxes Bot - features ‘CoronaVirus.apk’ as its file name. The malware is a remotely controlled mobile banking Trojan with ransomware functionality. It masquerades as a Google Update and displays a ransom note with a Russian email address. Victims so far have been located in Turkey, Iceland, Spain, Russia, and the US. [9]

# Fraud

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

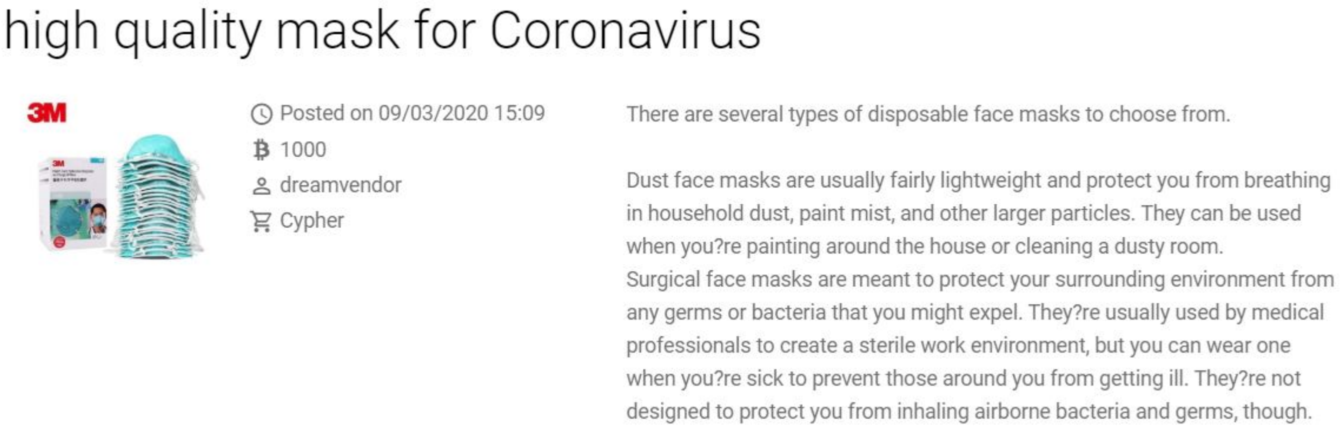
WHO, requesting funds in Bitcoin to access essential information. Investment scams, advising people to profit from the coronavirus downturn, have also been reported. [1]

Coronavirus-related scams are also being orchestrated by telephone and SMS. On 25 March, communications regulator Ofcom warned that fraudsters were calling and sending text messages claiming to be from the government, GP surgeries, the NHS and the WHO. The calls comprised an automated message or caller claiming to offer a test for the virus, treatment or cure, or to discuss the victim's medical needs. A human scammer will likely attempt to extract sensitive personal and financial information. The recorded messages ask the recipient to press a button on the phone, transferring them to a premium-rate number. The SMS messages primarily contain a link to a malicious website that harvests credentials or disseminates malware. [2]

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. [3] The sale of fake coronavirus testing kits is also a concern. Some of these have contained purified water vials valued at nearly $200. [4] 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. [5] 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 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. [6] Thankfully, many distilleries have begun producing hand sanitiser alongside their usual products, helping to bolster supplies. [7]

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". [8] 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.



high quality mask for Coronavirus

Posted on 09/03/2020 15:09
₿ 1000
dreamvendor
Cypher

There are several types of disposable face masks to choose from.

Dust face masks are usually fairly lightweight and protect you from breathing in household dust, paint mist, and other larger particles. They can be used when you?re painting around the house or cleaning a dusty room.
Surgical face masks are meant to protect your surrounding environment from any germs or bacteria that you might expel. They?re usually used by medical professionals to create a sterile work environment, but you can wear one when you?re sick to prevent those around you from getting ill. They?re not designed to protect you from inhaling airborne bacteria and germs, though.

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]
- Cybercriminals are spoofing official UK government phone numbers and using them to trick users into disclosing their bank details. Some of the threat actors actually managed to hijack the thread of an official UK government coronavirus alert service. Those contacting the service are told they must pay a fine of £35 having been observed leaving their home on three occasions. Another version of the scam claimed the caller was owed a £258 'goodwill payment' from HMRC. Many different versions of these scams have been seen. [3]
- Sextortionists are emailing victims claiming to have stolen an explicit video of them. The long-running scam has been updated to include a threat that the victim's entire family will be infected with coronavirus if they do not comply. [4]

# 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
- 76387fb419cebcfb4b2b42e6dc544e8b
- 55b75cf1235c3345a62f79d8c824c571
- 030e95d974c5026499ca159055b2dfa6
- bc466506e3f184c45054c93445275d9b8ef044f8
- 54afa3a4e2ca8ac91c4f54641e267c78d58948b9
- afabf51065d63ea7edc95af3c8548ad774321202
- f224fc2f1a2ce1e3e1d1ff9d194405e99157725e
- CBB32307586F83D070BB84AD6C26DD73
- C8DFF758FEB96878F578ADF66B654CD7

- 70E58943AC83F5D6467E5E173EC66B28
- 7CA44F6F8030DF33ADA36EB35649BE71
- 8A96E96113FB9DC47C286263289BD667
- C6D279AC30D0A60D22C4981037580939
- BBDD27E2EC52728930A920D8E926A8666DDC9F0D
- c844992d3f4eecb5369533ff96d7de6a05b19fe5f5809ceb1546a3f801654890
- b41e2237590421056f41a33b004670abf29dc83157b1f38c0eab65ecfd6b9663
- 6b61c223d618ead7ca78f4731a0128e30bf602bdfe8d940e442041486cb2fe76
- 58e918466a61740abe42a2d1ca29bd8d56daf53912e6d65879cbe944466fb80c
- 8e3240a2a6b07ae8a6fde884c0e18e476ca3e92438022fe1a1ad4b2ba2334737
- 1b93ca543c1e7ad43363e087059bb0e48ed134a2ee8cb0902be23a8a86e7656b
- 345d8b4c0479d97440926471c2a8bed43162a3d75be12422c1c410f5ec90acd9
- 9fa1f8cb9822b7de436cbeba95ddce241c2510e03825c02f21705922e77c40a2
- dd7023dd82b641c9307566b87acf0951f16b27c34094a341fa1fe7671d269bf4
- 8a9feda526489531ffb275a88b4c70bf7fe92c7807503c3654cf926ff9bb7d85
- 955352b5116d7de50dc75377889a495446554779fb768260be4b23c59a5a967e
- 7e52f7a7645ea5495196d482f7630e5b3cd277576d0faf1447d130224f937b05
- 5987a6e42c3412086b7c9067dc25f1aaa659b2b123581899e9df92cb7907a3ed
- 3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3
- 22b08d49f76e9310740928b386deb333c5b595706ca6afc3c7d0b3cc2635182a
- 2ec4d4c384fe93bbe24f9a6e2451ba7f9c179ff8d18494c35ed1e92fe129e7fa
- 2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
- da26ba1e13ce4702bd5154789ce1a699ba206c12021d9823380febd795f5b002
- 51eab875208923d82953fd3492b2efab3dc1d234c555a2db9dcd45e840a9040c
- 4daf1f057fb07090d760ae527f7401ad7224a27881824c714743ac29450add84
- f5b214cb8d7bcf9b6baea0f971e42be1064a2636984381ed0fd8bbdfe6800188
- b41e2237590421056f41a33b004670abf29dc83157b1f38c0eab65ecfd6b9663
- 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
- 146dd15ab549f6a0691c3a728602ce283825b361aa825521252c94e4a8bd94b4
- 6A22EEA26C63F98763AA965D1E4C55A70D5ADF0E29678511CF303CB612395DF0
- e2794482a495d01c1c9c244dc059f123d6d8cb3d024dfbb9864d7c80ab917da6
- 93288d18a7b43661a17f96955abb281e61df450ba2e4c7840ce9fd0e17ab8f77
- 889392ed44a613bb3618f6b9a05a663f801c9cd7086ff8d3d7531c3bc57d97be
- d5239210a9bc0383f569e9ca095fe8bdfb9a482bc0c77c8658fcecb23b8a26bc
- 575890d6f606064a5d31b33743e05654b9ed9200758a9802491286c6a313139a
- 07c30054c7c22b8b53638367c4c3ad484a1a336b615e1a6944260d5ec797a66a
- 23e8884c69176d5cf4da0260cdbb296301c0e0afccd473d57033ac1a06f227c3
- 51d7ebd3af38432c68c913aef48fe26a206fda4b52c9f09728df69cab13a4b3b
- 1c0316d0194e8008904679242d592d1a2aeeb2bacef28c7854e4361692a085e7
- 6caa6342caefe3fea23353e850cb2c974e8607c017661b7410de7a10004b05ec
- f3f14cdada70d49c3e381cc1b0586018e6b983af8799d3e6c4bee3494c40e1d6
- 3c1bfbdfae91f1f248180c2102ed65fbdec086a334193894db67b0461a0485c5
- 1eec0e1ebeefc6667b6ee08e8dede5cd36ca10697180f10e2d43a2fdebbeefcb
- 650a5958a06b16aa819e4e86858746750b8c72a75f31bfdfb6b47fd38d72b602
- 0dfec52076249d91ec623ea52177352fbc8fb258db316eac85462c7b459f1a2d
- 641d22e38b4135c56b7fb6037a6d76098ffae9e84664993a3f4c07859b77241e
- 4887389ffaf4257b37408eac9f1740eabe805f830009cf58185757372f903667
- ce5241de3a378a64266c56fe5094ecbb8baa7afd677a3112db8074db78a55df1
- 3135efd29cb8b0fab961ddd7ec99e148dc4c5cca6c3303d60192dc9664849545
- 54c27a8b48b96e63402698d3bba41480a815d103c92084d467d3c664eec0a7f8
- 3163c8b8deb3cdda9636c87379b1c384dec207ce9f15f503ffb4b1ef8cfab945
- DFF2E1A0B80C26D413E9D4F96031019CE4567607E0231A80D0EE
- 238a1d2be44b684f5fe848081ba4c3e6ff821917
- 69a6b43b5f63030938c578eec05993eb
- a4388c4d0588cd3d8a607594347663e0
- 1b6d8837c21093e4b1c92d5d98a40ed4

- 4008eec5413e2cf20bb1d6d039d027fdab6e0283
- bda2e2ba4e4deb14b27fb6e52f255dfebf7bdbfa
- 599db33d534d1e98ea63dd2ce30100a7
- 07d0be79be38ecb8c7b1c80ab0bd8344
- 05adf4a08f16776ee0b1c271713a7880
- ef07feae7c00a550f97ed4824862c459
- FDB2F4EFA95DD8B5EAD7527C92F24542
- 4202C9E8835552CD64F6A978FDF6BAAB
- A9DAC36EFD7C99DC5EF8E1BF24C2D747
- 5F2D3ED67A577526FCBD9A154F522CCE
- A4388C4D0588CD3D8A607594347663E0
- 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
- 104.27.179[.]176
- 104.27.178[.]176
- 185.14.29[.]227
- 49.51.161[.]225
- 47.254.174[.]129
- 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

- hxxp://newbot[.]ug
- 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
- hxxps://promo-covid19-neftlix[.]ml
- hxxp://testtesttest.cloud/language/wschramm2001[.]php
- hxxp://coronasafetymask[.]tk
- hxxp://coronavirusapp[.]site
- hxxp://uk-covid-19-relieve[.]com
- hxxp://thanhxuanvietcom/ktzoq9aicz/williamwoo1668[.]php
- hxxps://corona-map-data[.]com/bin/regsrtjser346.exe
- hxxps://bitbucket[.]org/example123321/download/downloads/foldingathomeapp.exe
- hxxp://ambesagar.choicegroup[dot]co/cgi-bin/williamlrobertson.php?t=VHVlLCAxNyBNYXIgMjAyMCAwMDoxMjo0OCArMDMwMA==
- 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
- hxxp://185.62.188[.]204/hunt/post/corona[.]exe
- hxxps://coronaviruscovid19-information[.]com/en/
- hxxps://coronaviruscovid19-information[.]com/tr/
- hxxps://paypaluk-coronavirussupport.com
- 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
- hxxps://antivirus-covid19[.]site
- hxxps://corona-apps[.]com/Corona-Apps.apk
- hxxp://corona-apps[.]com/Corona-Apps.apk
- hxxps://corona-apps[.]com/
- hxxp://corona-apps[.]com/
- hxxp://getegroup.com/file[.]exe
- hxxps://seobrooke[.com]
- hxxps://securitysystemswap[.com]
- hxxps://axelerode[.club]
- hxxp://brinchil[.]xyz
- instaboom-hello[.]site
- dw.adyboh[.]com
- wy.adyboh[.]com
- feb.kkooppt[.]com

- compdate.my03[.]com
- jocoly.esvnpe[.]com
- botduke1.ug
- t.me/botduke1
- 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
- vnext[.]mireene[.]com
- nhpurumy[.]mireene[.]com
- mybobo[.]mygamesonline[.]org
- crphone[.]mireene[.]com
- www.messager[.]cloud
- news2.hkrevolution[.]club
- news.hkrevolt[.]com
- app.hkrevolution[.]club
- app.poorgoddaay[.]com
- appledaily.googlephoto[.]vip
- news.hkrevolution[.]club
- www.facebooktoday[.]cc
- www.googlephoto[.]vip
- svr.hkrevolution[.]club
- phantom101.duckdns.org:5200

## 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 Limited
6 Mitre Passage
Greenwich
London SE10 0ER

info@cyjax.com
+44 (0)20 7096 0668
CYJAX.COM