CYJAX

Digital Intelligence
Securing the Future

COVID-19 Critical Infrastructure Cyber Threat Brief

CLIENT CONFIDENTIAL

Purpose

This Cyber Threat Brief is intended to help mitigate the risk of cyberattacks against UK critical infrastructure during the coronavirus pandemic. We have defined critical infrastructure as: food supplies, medical supplies, transportation, security services, telecommunications, utilities and financial services. This report provides a broad overview of all relevant coronavirus-related digital threats, alongside more general vulnerabilities that attackers could exploit. We at Cyjax hope this will help organisations and their staff protect themselves from digital threats during this national crisis. If you require any further assistance or advice, please contact us.

Overview of malicious cyber activity

We have witnessed a significant uptick in cyberattacks exploiting fear of the coronavirus to compromise victims. Notably, however, there has not been a surge in the total number of attacks. Instead, existing cybercriminal operations have been rethemed with COVID-19 lures. Attackers have not gained more resources, but are instead repurposing their existing phishing, ransomware, and malware infrastructure to include COVID-19-themed keywords in a bid to infect more users. [1]

All sectors are being targeted with COVID-19-themed attacks, including those operating in the critical infrastructure space. Attacks have ranged from generic “spray and pray” attacks to highly targeted advanced persistent threat (APT) operations. A broad array of nation-state actors have been involved from China, Russia, North Korea and Iran, among others. Sophisticated cybercriminals are also staging coronavirus-themed attacks. Most notably, organised ransomware gangs, who have continued to compromise, encrypt and leak data from a diverse group of organisations.

Coronavirus-themed malicious emails are predominantly delivering phishing links. However, a variety of malware is also being disseminated. This includes the AgentTesla keylogger, Ave_Maria stealer, Black RAT, FormGrabber, Hakbit ransomware, Hawkeye keylogger, KPOT infostealer, LimeRAT, LikiBot infostealer, NanoCore RAT, Nemty ransomware, Pony, Remcos RAT, SalityBot and TrickBot, among others. Many of the emails impersonate legitimate organisations, such as the World Health Organization (WHO), Centres for Disease Control (CDC) and other healthcare bodies. [2]

The scale of the threat is vast: GMail's in-built malware scanners blocked around 18 million phishing and malware emails using COVID-19 lures in a single week. [3] The prevalence of coronavirus-themed attacks has sparked cooperative action from British and American cybersecurity bodies. On 8 April, US-CERT, CISA, and the UK NCSC issued a joint security advisory, warning of an increase in COVID-19 related themes by malicious actors for SMiShing, phishing for credential theft, and phishing for malware deployment. US-CERT's report can be found here. The full security advisory from the NCSC can be found here.

The unprecedented shift to remote working has compounded the risk of malicious cyber-attacks and accidental breaches. According to a study of 41,000 companies, many of the millions of home workers are using malware-infected work from home and remote office (WFH-RO) networks. These networks are were found to be 3.5 times more likely to be infected. Indeed, 45% of companies were found to have malware on their employees’ work from home networks. [4]

Disinformation, misinformation and conspiracy theories are rife. The situation has become so serious that the WHO declared an "infodemic" and warned of the potential impact on global health. [5] 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. One of the more outlandish conspiracy theories linked 5G networks to the coronavirus pandemic. Despite numerous official sources stating that the allegations are false, the rumours have had

significant real-world consequences. Across the UK, activists have set fire to what they believed were 5G masts at over 20 locations. [6]

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. [7] Elsewhere, there have been reports of fake decontamination services being sold, as well as counterfeit coronavirus testing kits, medicines and protective equipment. [8] 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.

Firms operating in the critical infrastructure sector are by definition vital to national security. Consequently, it is essential that all possible steps are taken to protect the operational capacity of these key organisations from coronavirus-themed attacks. Cyjax can help ensure that staff are aware of emerging digital threats and understand how to protect themselves and their employers. This will significantly reduce the likelihood of a successful attack, protecting the organisations and the millions of British citizens that rely on them.

APT Activity

An Advanced Persistent Threat (APT) is a skilled offensive cyber group, usually backed or directed by a nation-state. These groups conduct hacking operations to bolster national security and/or gain commercial advantages in key industries. Consequently, organisations operating in the critical infrastructure space present an attractive target to APTs, as they hold information that fulfils both of these criteria. In this section, we have also included details of any organised attack groups that present a significant threat to the critical infrastructure sector.

A broad range of APT groups are deploying coronavirus-themed attacks to compromise victims. In the US, the FBI has evidence of foreign state-sponsored hackers attempting to break into US COVID-19 research institutions, some of which were successful. Organisations make themselves a target by publicly announcing the results of their research. This can pique the interest of foreign actors intending to glean details about their operations and potentially steal proprietary information. (1, 2)

Numerous Chinese APTs have been observed using coronavirus-themed lures in their attacks, including MustangPanda, ViciousPanda and EmissaryPanda. [3, 4, 5] 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.

Another Chinese state actor, APT41, has been observed engaging in a likely targeted global intrusion campaign since early 2020. It is one of the broadest Chinese cyber-espionage operations in recent years. Between 20 January and 11 March, APT41 attempted to exploit vulnerabilities in Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central at over 75 different organisations. The UK was among several targeted countries, including Australia, Canada, Denmark, Finland, France, India, Italy, Japan, Malaysia, Mexico, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, UAE, and the USA. The following critical infrastructure sectors were among those targeted: banking/finance, construction, defence, government, healthcare, education, manufacturing, oil & gas, pharmaceutical, telecommunications, transportation, and utilities. [6]

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". [7] The group has previously targeted British organisations operating in the energy, aviation, healthcare, finance, manufacturing, transportation and government sectors. [8] Consequently, it is likely that the group will target the UK critical infrastructure with COVID-19-themed attacks in the near term.

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. [9] However, it does underscore the potential of a similar disruptive DDoS attack against an essential service in the UK.

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. [10] 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. Cyjax's Domain Monitor tool can help protect against these types of attacks. By monitoring typo-squatted domains as they are registered, we can proactively identify counterfeit sites impersonating essential services, initiate takedown proceedings and disrupt the threat actor's operation before it begins.

Organised ransomware gangs continue to present a significant threat to businesses in all sectors, including critical infrastructure. Groups including Maze, Doppelpaymer, Sodinikobi/REvil, Pwndlocker, Ako and Nefilim have infected a broad range of organisations, encrypting their systems and then publicly leaking data if a ransom is not paid. Victims have been diverse, indicating some level of opportunism in the attacks. These have included: Boom Construction Company, a Qatari contractor that services the water, road and utility sectors [11]; Cognizant, one of the world's biggest IT service providers [12]; UAE-based petroleum and industrial supplier LIWA National Engineering [13]; US grocery retailer C&K Market and Berkine, a petroleum joint venture between the Algerian Sonatrach and the American Anadarko Petroleum Corporation through its subsidiary Anadarko Algeria Company LLC. [14]

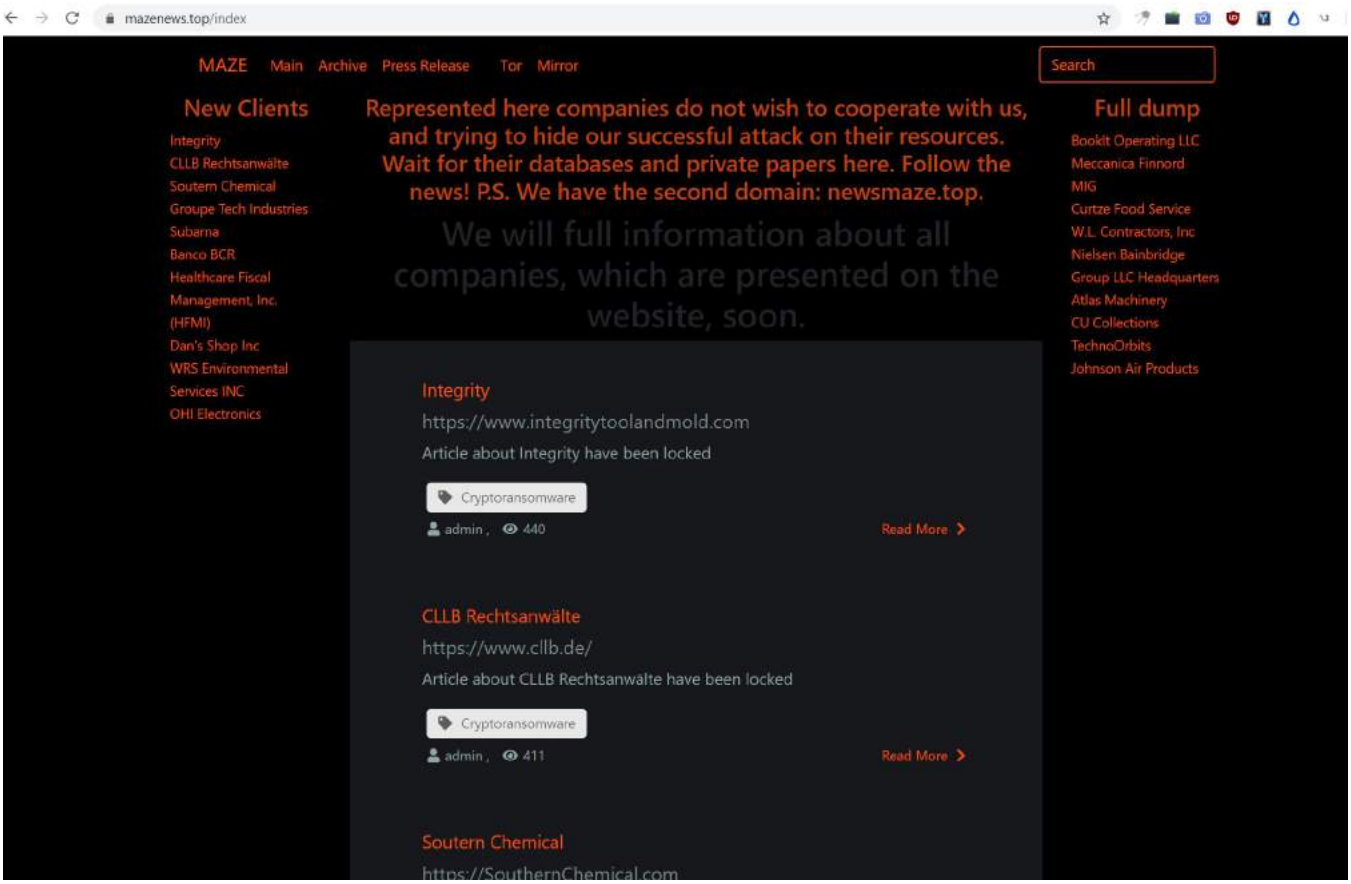

Fig. 1 - Maze ransomware leak site

Interestingly, the ransomware groups have responded differently to the coronavirus pandemic. Maze and Doppelpaymer pledged to avoid targeting healthcare organisations until the situation improves. Despite this, UK-based Hammersmith Medicines Research was infected with Maze ransomware on 16 March. Fortunately, the company was able to repel the attack and quickly restore all functions. [15] In contrast, the REvil group appears to be purposely targeting stretched healthcare organisations, as are the Ryuk ransomware attackers. Ryuk is traditionally delivered by TrickBot, one of the most prominent malware being distributed during the pandemic. Consequently, any organisation infected with the Trojan should initiate incident response proceedings immediately to reduce the likelihood of a subsequent ransomware infection. [16]

Organised ransomware groups use various methods to infect victims, including phishing emails and brute-forcing public-facing RDP clients. Some are also scanning the internet for vulnerable gateway and VPN appliances to exploit. REvil has previously targeted flaws in Citrix ADC and Gateway products, as well as vulnerabilities in the Pulse Secure VPN platform that was used to compromise Travelex last year. In the run-up to these types of ransomware attacks, adversaries typically persist on networks, undetected, for long periods only to deploy the main payload later. This type of ransomware is harder to remediate due to incident responders having to identify the initial intrusion and determine the extent of the infection. Further, they are human-operated, instead of generic ransomware-as-a-service (RaaS) attacks. Consequently, the threat actors use their technical expertise to exploit security misconfigurations and vulnerabilities. As such, it is important to patch systems promptly, monitor remote access carefully, turn on attack surface reduction rules in Windows, and switch on AMSI for Office VBA in Office 365 environments. [17]

Coronavirus-themed APT attacks are almost certain to continue targeting the UK critical infrastructure sector in the near term at least. As such, it is essential that organisations maintain visibility on emerging APT campaigns targeting

these organisations. Cyjax can help in this regard by providing timely, accurate and actionable cyber threat intelligence. Critical vulnerabilities can thus be patched before a threat actor is able to identify and exploit them. Additionally, understanding a group's tactics, techniques and procedures (TTPs) will allow organisations to respond proactively, implementing effective mitigations that will further minimise the likelihood of a successful breach.

Malspam

There has been a significant uptick in malicious emails using coronavirus-themed lures to disseminate malware. Recent findings indicate attackers sending approximately 1.5 million coronavirus-themed emails per day. [1] 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. Predominantly these messages are untargeted and distributed at scale to all sectors. However, there have also been numerous campaigns targeted at the critical infrastructure sector, some of which are detailed below.

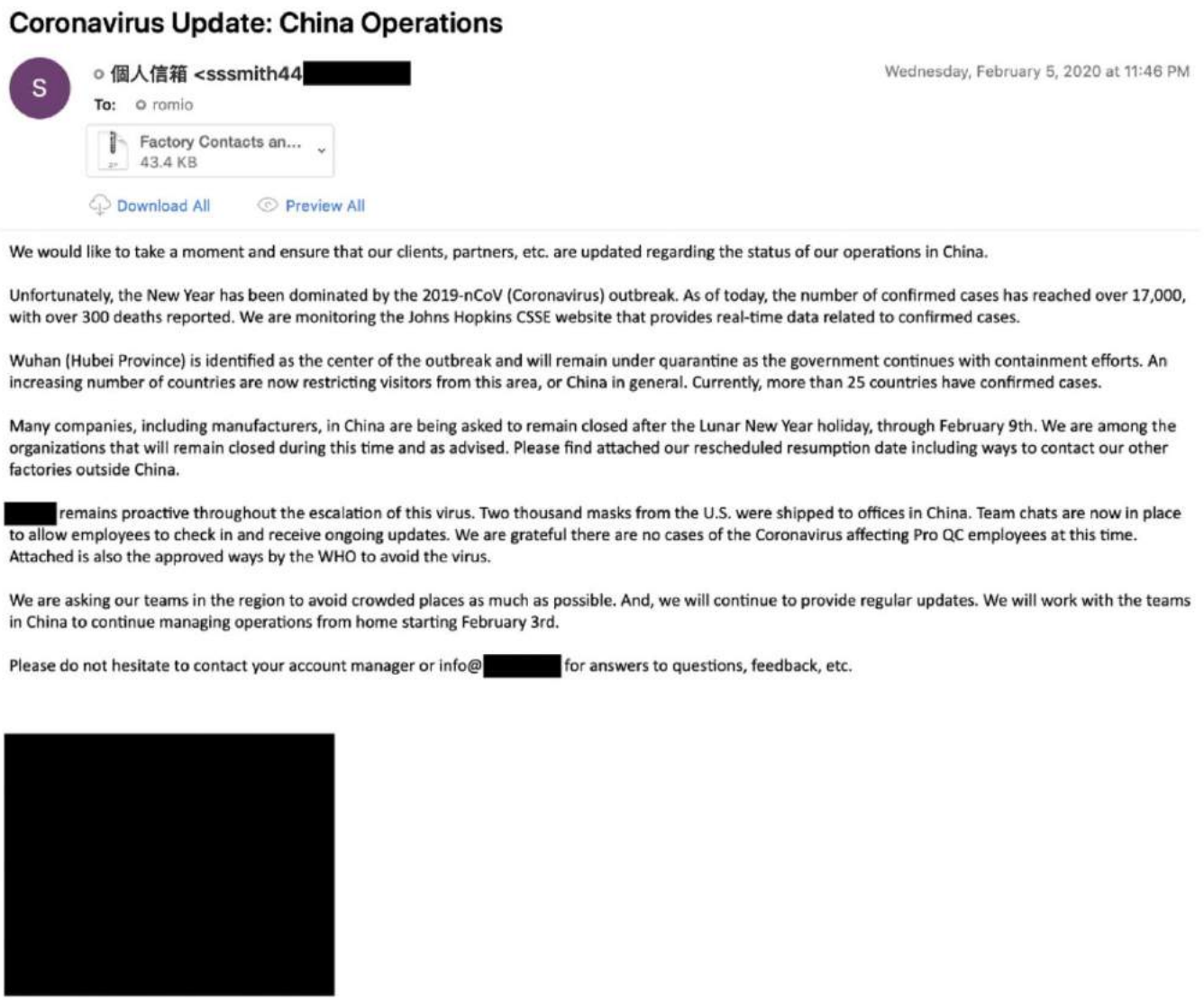

Fig.2 - Coronavirus-themed malspam

A diverse selection of malware is being delivered in coronavirus-themed malspam, including the TrickBot banking Trojan, Ostap downloader, Remcos RAT, Emotet, Nanocore RAT, Agent Tesla keylogger, Lokibot infostealer, Ryuk

ransomware, Hancitor Trojan and Bisonal malware, among others. According to analysis from Microsoft, TrickBot is the most prolific malware being distributed in coronavirus-themed lures. In one notable campaign, several hundred unique macro-laced attachments were disseminated in emails impersonating a non-profit offering free coronavirus testing. [2] As mentioned above, TrickBot does not only put the victim at risk of financial losses, it can also lead to a subsequent ransomware infection, compounding the risk.

Another banking Trojan, Grandoreiro, is being delivered in COVID-19-themed videos that trick users into running a concealed executable. Once infected, the remote-access tool notifies the attacker when a banking website is visited. As the victim accesses their account, the attacker can display full-screen overlay images that appear to be part of the genuine site. These may request additional information or block further interaction with the site, allowing the attacker to transfer funds from the account. The malware previously targeted Brazilian users but has since migrated to Spain without significant modification. [3] As such, it is possible that Grandoreiro campaign could target the UK banking sector in the near future.

Multiple organisations, including a chemicals company in the Czech Republic, have been targeted in an evasive coronavirus-themed Formbook campaign. Formbook is an infostealer that can capture the contents of the Windows clipboard, log keystrokes and steal browsing data. It can also execute commands from a command and control (C2) server. These include downloading and executing files, starting processes, shutting down and rebooting the system, stealing cookies and local passwords. The campaign leverages two vulnerabilities, CVE-2019-9621 and CVE-2019-9670, to enable a Server Side Request Forgery (SSRF) exploit that allows unauthenticated remote command execution. [4] Consequently, organisations should patch these two vulnerabilities as a priority.

LokiBot, another long-running infostealer and keylogger, is also being distributed in COVID-19 and WHO-themed phishing emails. LokiBot is sold on underground forums and aims to collect credentials from multiple applications, such as Mozilla Firefox, Google Chrome, Thunderbird, FTP, and SFTP applications. The emails deliver malicious documents that leverage the CVE-2017-11882 (Office Equation Editor) exploit via malicious RTF files. This campaign is indiscriminate, targeting all sectors, including critical infrastructure. Victims have been identified in Turkey, the US and Canada, alongside multiple other European countries. [5]

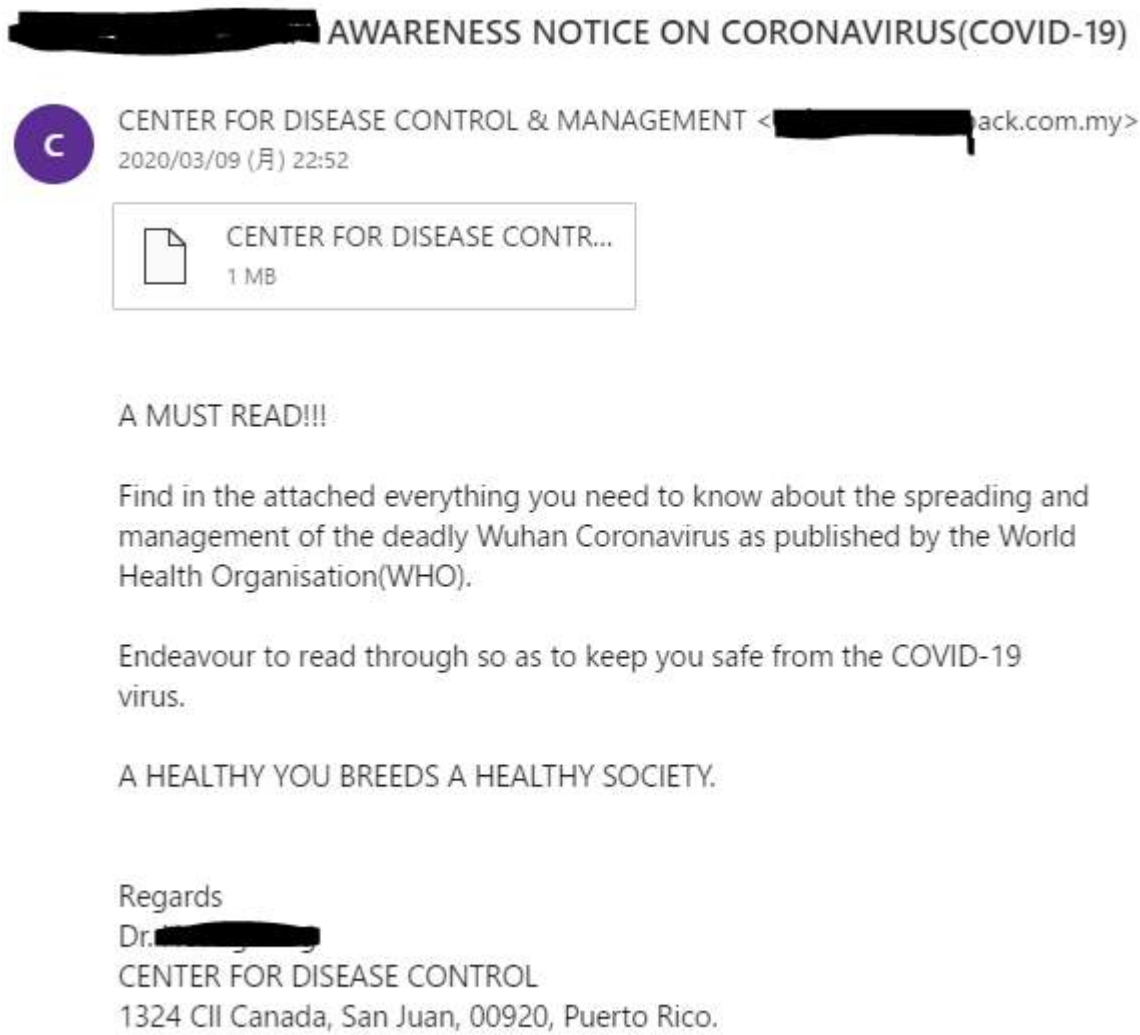

Fig.3 - CDC malspam delivers LokiBot

Elsewhere, the WarZone RAT is being delivered in COVID-19 themed phishing emails. WarZone is a malware-as-a-service (MaaS) that is sold on the darknet. It has multiple features, including the ability to remotely control the victim's webcam, exfiltrate passwords, access files and download and execute arbitrary code. In this latest campaign, 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. [6] Notably, this vulnerability was patched in November 2017, significantly reducing the attack surface. [7]

That being said, many organisations remain vulnerable to long-patched vulnerabilities that are being actively exploited. A recent campaign that relies heavily on COVID-19-themed malspam is pushing an EternalBlue downloader Trojan. This is delivered via the recently discovered BlueTea worm. The subject of the email is typically "The Truth of COVID-19". It contains a malicious RTF document that exploits CVE-2017-8570, a Microsoft Office RCE vulnerability that was also patched in November 2017. Due to many organisations failing to update their systems, the EternalBlue vulnerability is still able to be compromised by malware if systems are exposed to the public-facing internet. [8]

While many COVID-19-themed malspam operations are untargeted, some have focused on particular sectors, most notably healthcare. A campaign targeting hospitals and manufacturing facilities in the US 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. It can steal login credentials, cookies, autocomplete fields and credit cards details, among other information. [9] Another campaign targeting similar victims purported to provide information for treating or curing the virus. Instead, recipients were infected with the HawkEye infostealer malware via malicious RTF documents. [10]

Numerous campaigns have exploited the financial hardship faced by many people using lures that claim to offer assistance or information about government grants. A recent scam impersonating "Jim Harra, First Permanent Secretary and Chief Executive of HMRC" invited recipients to make a financial claim under the UK government's legitimate Coronavirus Job Retention Scheme. The victim is asked to provide their bank account details in order to receive payment: the data is then stolen. At least 50 UK businesses received the emails. [11] Another campaign referenced a "Stimulus Package" and contained a malicious attachment. [12] When users open the file, they are infected with the AgentTesla infostealer. AgentTesla is a popular malware-as-a-service offering that has been infecting users since 2014. It is capable of extracting credentials from browsers, mail and FTP clients, while also logging keys, clipboard data, form-grabbing, capturing screenshots and recording video. [13]

AgentTesla remains a pervasive threat to the critical infrastructure sector. On 21 April, two spear-phishing campaigns were identified that were targeting oil and gas firms in multiple countries, including Malaysia, the US, Iran, South Africa, Oman and Turkey. While the oil and gas sectors were the main targets, other verticals which have been flagged as 'critical' during the coronavirus pandemic have also been targeted. These include charcoal processing, hydraulic plants, manufacturers of raw materials, and transporters of large merchandise. [14] Another campaign AgentTesla campaign leveraging the virus has targeted a US defence research entity, a Turkish government agency, a German industrial manufacturing firm, a Korean chemical manufacturer, a research institute located in Japan and other medical research facilities in Canada. [15]

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, other major healthcare organisations and government departments will continue to be spoofed as people seek updated information on the coronavirus. Unfortunately, these campaigns are often effective. A recent study found that around 60% of respondents would share personal details, including banking details, with healthcare services and government agencies. [16] As such, it is vital that users exercise vigilance and avoid opening emails that appear to have come from an official source.

Malicious Websites

There has been a significant increase in suspicious coronavirus-themed domains registered in the past few months. Estimates vary, but since January 2020, tens of thousands of domains have been created using terms such as ‘corona’, ‘covid’, ‘epidemic’, ‘pandemic’, and 'Wuhan'. [1] In one study, approximately 3% of the domains were confirmed as malicious and 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. [2] The situation has become so dire, many hosting providers have halted the automatic registration of website names that reference the COVID-19 health crisis. [3]

Some of the domains host 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. [4] Similar pages have also distributed the DanaBot banking trojan, [5] or installed a backdoor in the target system via a fake Adobe Flash Player Update. [6] In one instance, a fake "Public Health Agency of Canada" website distributed a malicious Word document that dropped the Ursnif (Gozi) banking Trojan [7]. All of these malware are designed to capture sensitive victim information, including logins for banks, email accounts and social media platforms.

Fake government sites have also become an effective way to defraud victims. Threat actors stole millions of euros in emergency aid from the government of North Rhine-Westphalia (NRW), Germany, by creating a counterfeit version of the official website used to distribute COVID-19 financial aid by the NRW Ministry of Economic Affairs. The phishing pages were distributed through email campaigns and used to collect details of local residents. Using the stolen data, the threat actors filed requests for government aid on behalf of the victims, diverting the funds to an account controlled by the criminals. [8]

Standard phishing pages are also being delivered in coronavirus-themed emails. In many instances, these are untargeted and distributed in bulk to potential victims. Standard UK government phishing websites have also been modified to offer the promise of COVID-19 aid or relief. Others have targeted essential workers. 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. [9]

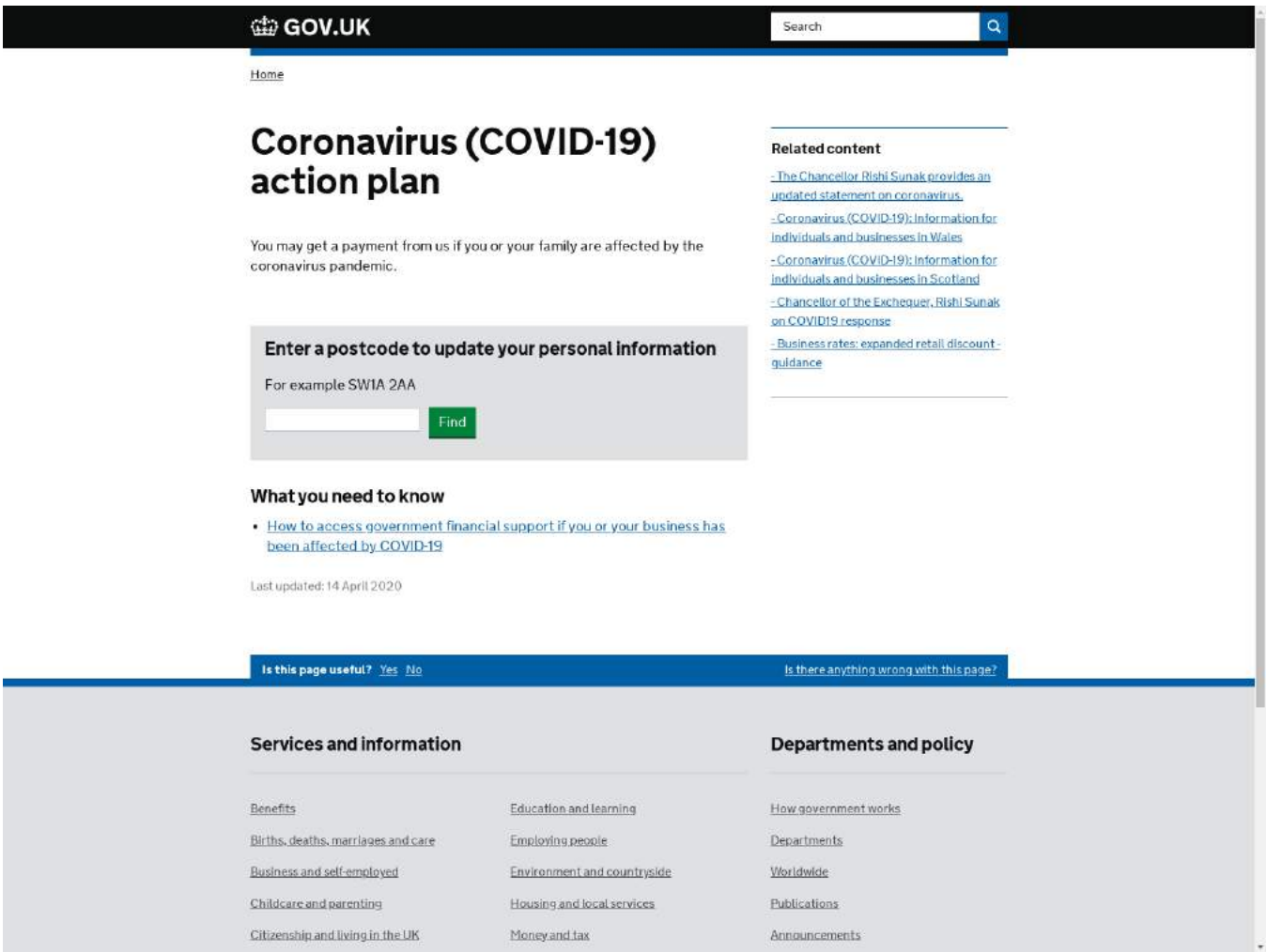

Fig.4 - UK government COVID-19-themed phishing page

Despite efforts by some hosts to tackle the spread of coronavirus-themed domains, we expect these to continue to proliferate in the near term. Many of these will impersonate national and supranational health bodies, including the CDC, 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, including critical infrastructure, 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.

Malicious Apps

As the pandemic has progressed, developers have begun disseminating malicious coronavirus-themed Android apps on Google Play and unofficial app stores. Initially, far fewer apps had been discovered than malicious domains, likely reflecting the time and effort that it takes to develop an app compared to creating a malicious website or launching a phishing campaign. However, as the pandemic has progressed, these have become increasingly prominent, presenting a threat to all sectors and the general public.

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. They abuse keywords associated with the pandemic, delivering ransomware, spyware, and more. [1] Android banking Trojans feature heavily among the apps. Several variants deliver Cerberus, 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. [2] Others called 'CoronaFinder.apk' or 'MediaPlayer.apk' feature a simple interface which shows the number of people infected near you and deliver the Ginp Android banking Trojan. (3, 4)

Fig.5 - Fake COVID-19 tracking app delivers Cerberus banking Trojan

Another new mobile banking Trojan - Android Xerxes Bot - features 'CoronaVirus.apk' as its file name. The malware has ransomware functionality and masquerades as a Google Update, displaying a ransom note with a Russian email address after infection. Victims so far have been located in Turkey, Iceland, Spain, Russia, and the US. [5] A new Android spyware called SpyMax, was discovered on a fake pharmacy website referencing COVID-19 medicine. [6] Another notable example distributed 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. [7] Fortunately, researchers recently discovered a master password to unlock devices infected with CovidLock: 4865083501. [8]

As is the case with official COVID-19 websites, threat actors are also creating fake government apps. One example impersonated the Catalonian government's COVID-19 response mobile app [9]; another, the Italian social security and welfare institute (INPS). [10] Even official apps are presenting a risk to users. Vulnerabilities have been found in the official coronavirus applications of Colombia and Italy. The official Colombian COVID-19 app is government-sanctioned and has over 100,000 users. It was found to be revealing user data including Personal Health Information (PHI) and personally identifiable information (PII), both in plaintext. This included passwords and self-disclosed health information. The Italian app, which had been released in beta testing mode, had been recompiled with a backdoor and was actively infecting victims. [11]

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. Vulnerabilities in legitimate apps will continue to be discovered, as developers are pushed to release them quickly. 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.

Fraud

Scammers are increasingly exploiting fear of coronavirus to defraud victims. Since early February, Action Fraud has received hundreds of report of coronavirus-related fraud, resulting in collective losses of over £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] In the US, the Federal Trade Commission revealed that $12.78 million was lost to virus-related scams since January, with a median loss of $570 per scam. [2]

In April, the National Cyber Security Centre (NCSC) helped takedown 2,000 fraudulent online campaigns, including 471 shops selling fake coronavirus-related items and 832 advance-fee frauds where a large sum of money is promised in return for a set-up payment. [3] The same month, UK domain name registrar Nominet removed over 600 coronavirus scam sites. These websites were selling fake vaccines, protective equipment and frauds remedies related to coronavirus. [4] In The US, as of 21 April, the FBI's Internet Crime Complaint Center (IC3) has received and reviewed more than 3,600 complaints related to COVID-19 scams, many of which operated from websites that advertised fake vaccines and cures, operated fraudulent charity drives, delivered malware, or hosted various other types of scams. [5]

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. [6]

Another notable example involved cybercriminals 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 were 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. [7]

Instances of offline fraudsters impersonating NHS staff have also been uncovered. Several UK towns and cities have reported door-to-door scammers offering to help with shopping for payment or collecting donations to fund a vaccine. [8] The sale of fake coronavirus testing kits is also a concern. Some of these have contained purified water vials valued at nearly $200. [9] 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. [10] 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.

Fig.6 - Darknet vendor selling hydroxychloroquine tables - marketed as a cure for coronavirus

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". [11] Many of these are now being offered for sale on the darknet. One forum has even been offering the sale of blood from a person who claims to have recovered from the virus. [12] Some of the products on the darknet will be genuine, 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.

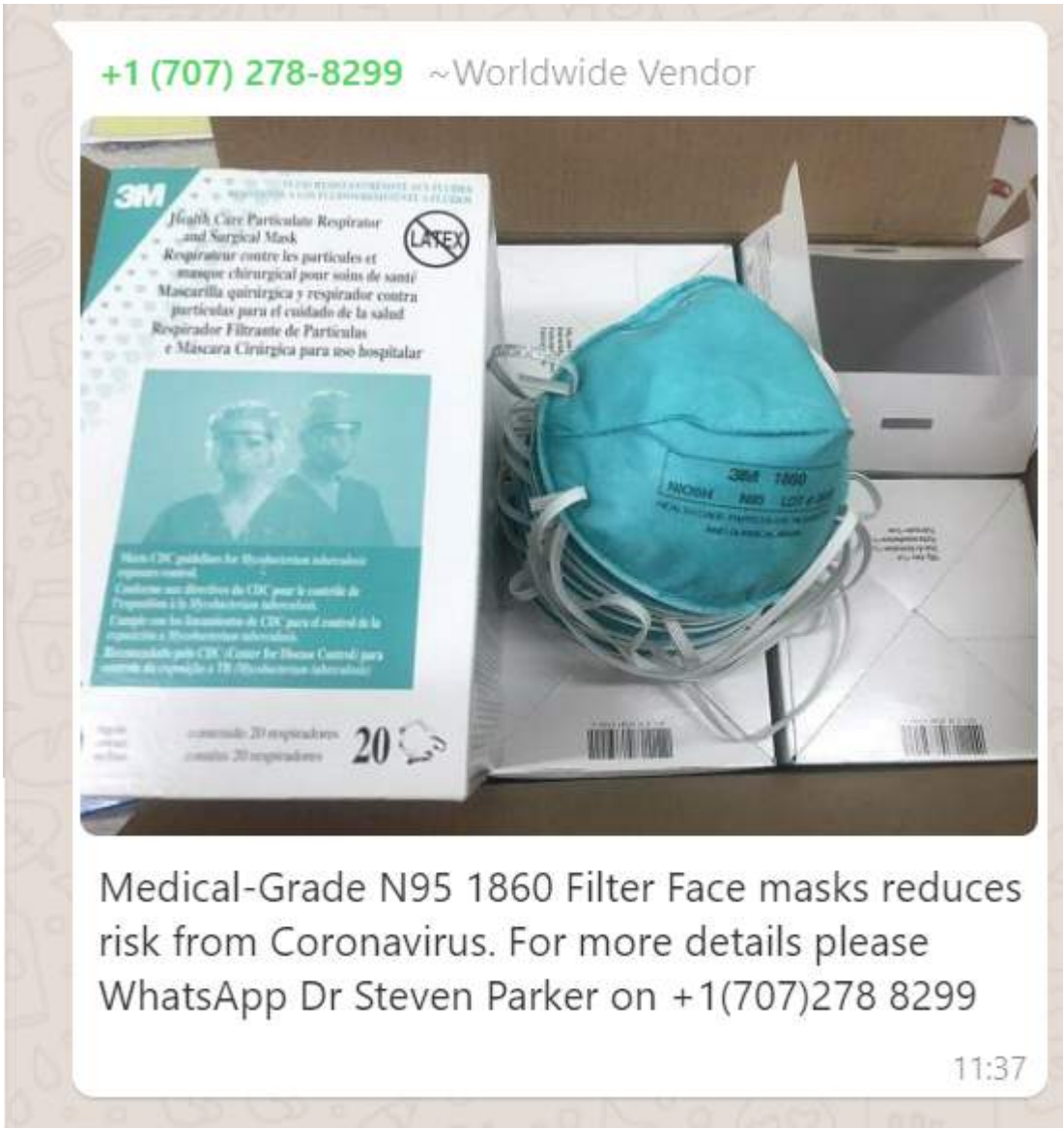

Fig.7 - Vendor advertising N95 face masks

The FBI has warned of an increase in coronavirus-themed business email compromise (BEC) attacks targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19. These attacks have also targeted financial institutions and banks. [13] In 2019, the FBI recorded 23,775 BEC incidents, resulting in more than $1.7bn in losses. [14] 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. [15]

BEC threat actors are now asking users for online gift cards in the midst of coronavirus-driven store closures. While there is a limit to the number of gift cards that can be bought in physical stores, there is often no limit to the amount of money that can be loaded onto an online gift card. Threat actors such as @ExaggeratedLion have been requesting as much as $15,000 in “surprise” gift cards, purportedly for the victim organisation's employees. [16]

Remote Working

The unprecedented shift to remote working has caused threat actors to shift focus to conference calling software. In a recent study of 1,300 suspicious files, 42% were disguised as Zoom, 22% as WebEx, 13% as GoToMeeting, 11% as Flock, and 11% as Slack. Zoom has been most targeted due to its popularity. Most commonly, threat actors are performing credential stuffing attacks to compromise accounts, which are subsequently gifted or sold on hacking forums. Cracking communities such as Cracked, Nulled and Raid Forums have all released configurations for common credential stuffing tools, such as Open Bullet. These configs are offered for free and allow anyone with the software to begin stealing Zoom accounts. In one notable instance, a database containing over 2,300 compromised Zoom credentials was leaked on the darknet. Victims included banks, consultancy companies, educational facilities, healthcare providers, and software vendors. [1]

In addition to credential stuffing attacks, threat actors have created thousands of new domains containing the word "Zoom" since January. Most commonly, these host Zoom phishing sites that intend to capture the visitor's personal details. Others offer the software for free download but also include other software such as InstallCore. These install unwanted software, bloatware, adware or malware onto the victim’s computer. In one instance, the Neshta file infector was repackaged with the installer. The programme’s interface is identical to the official app, and the certificate details are similar to the original. Another campaign targeted Zoom users with cryptocurrency mining Trojans. Users still receive a legitimate version of the Zoom installer, but the Trojan works in the background, hijacking resources to send mined virtual currency to the attackers. [2]

One of the most high-profile attacks is 'Zoom Bombing'. This practice involves pranksters joining unsecured Zoom uninvited, usually to display offensive content. There have been numerous high-profile incidents in recent months. On 10 April, for example, A US House Oversight Committee meeting discussing women’s rights in Afghanistan was disrupted three times by individuals who were not invited. It is not clear what the Zoom bombers did, or if any sensitive information was exposed while they were on the call. However, the incident did cause government officials to call for an immediate "suspension of any current or future use of Zoom systems for official committee activities and take immediate steps to evaluate the Committee’s internal cybersecurity preparedness to prevent hackers from accessing sensitive committee information through the Zoom platform.” [3]

Shortly after these attacks began, Cyjax identified a new public forum named 'Zoom Leaks'. The forum allows members to post the meeting IDs for unsecured Zoom meetings. In addition, an automated Zoom meeting discovery tool was discovered. The tool, zWarDial, gives threat actors the ability to find non-password protected Zoom meetings.

According to its creators, zWarDial can find an average of 110 meetings per hour. Each Zoom call is assigned a meeting ID which consists of 9 to 11 digits. Threat actors have now discovered that they can guess or automate the IDs with the correct number of digits. Researchers were able to do this in 2019 with a 4% success rate. [4] To mitigate the chances of these attacks, users should password protect all Zoom-based meetings.

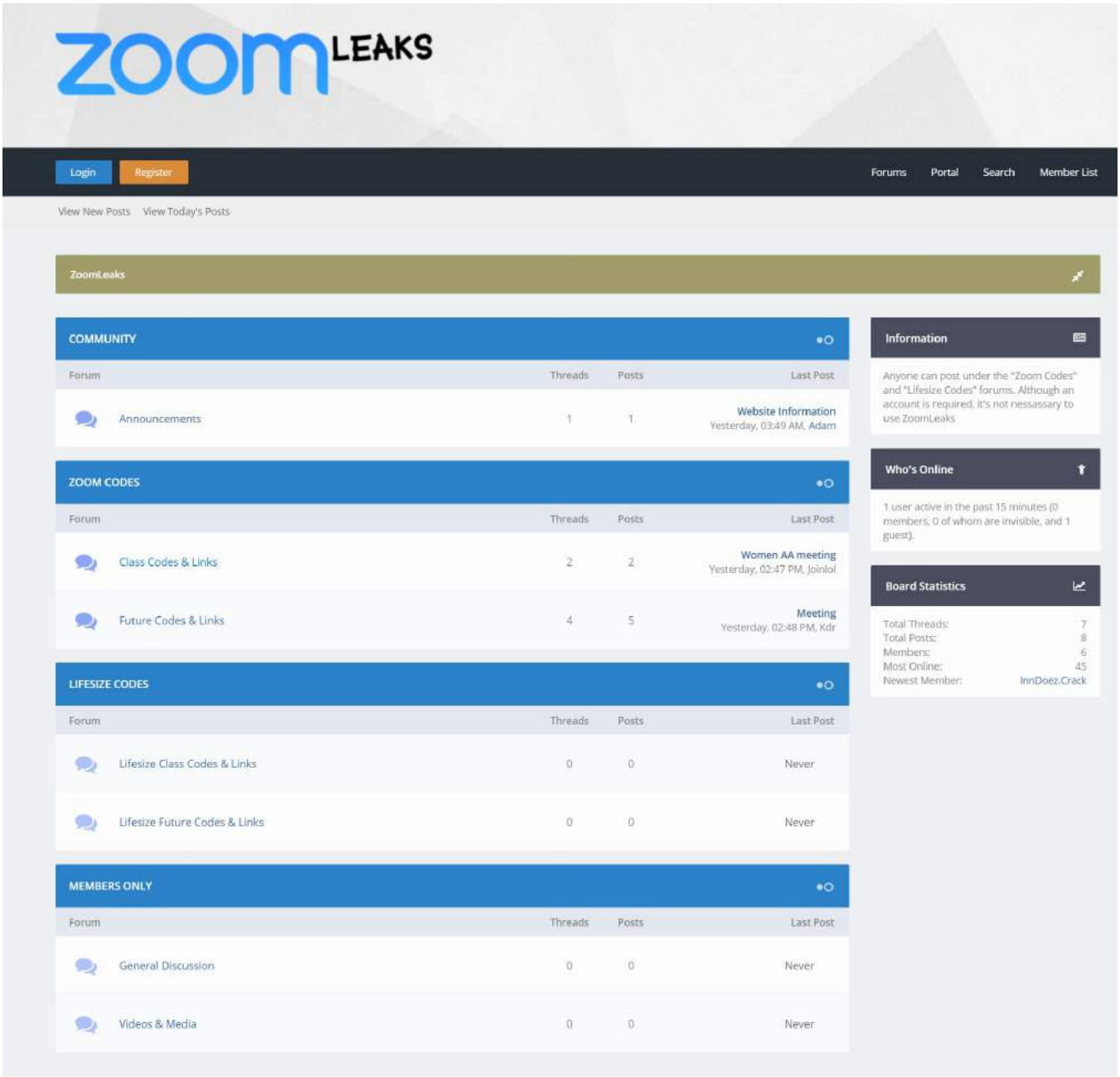

Fig.8 - Zoom Leaks forum

Accidental exposures of recorded Zoom meetings have also been a concern. In recent weeks, thousands of recorded Zoom meetings were found exposed on the internet without any password protection. These included private business discussions, meetings, therapy sessions, conversations between friends, and sexual content. Most of the recordings appear to have been made public by mistake. The problem lies in the file-naming convention used by Zoom to label recorded meetings. The service allows users to save their calls and recordings with a default file name. This, combined with a user accidentally uploading the private file to the internet from their computer, allows them to be easily

discovered. 15,000 exposed videos were discovered by a security researcher following a scan of unsecured cloud storage. Searching the Zoom file name on YouTube, Google, and Vimeo also reveals thousands of these videos. [5]

Several Zoom vulnerabilities have generated a significant amount of media exposure. A security researcher identified a vulnerability in the Zoom client's chat feature that leaves the user vulnerable to UNC path injection attacks. Within the chat feature, any URLs that are sent between participants are converted into hyperlinks, including Windows networking UNC paths. If a user clicks on a malicious UNC path link, Windows will attempt to connect to the remote server using the SMB file-sharing protocol. When the connection is made, the user's login name and NTLM password hash are sent by default - this can be cracked using free and readily available tools. In order to fix the vulnerability, Zoom clients would need to prevent the conversion of UNC paths into clickable hyperlinks. Users can enable the 'Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers' group policy to prevent NTML credentials from being shared. [6]

Two new 0day vulnerabilities were also discovered in Zoom's macOS client version which could give unprivileged attackers root privileges. The first flaw is a problem with the Zoom installers and can give an unauthorised actor root privileges to the application. The other vulnerability gives attackers access to the microphone and camera on the device. The first issue stems from the fact that the installer uses the AuthorizationExecuteWithPrivileges application programming interface (API) function to install the app without any user interaction. This API has been deprecated by Apple because it does not validate the binary being executed at root. To exploit the flaw, an attacker would simply have to modify the binary to include the 'runwithroot' script during an install. In the second case, if a malicious third-party library is loaded into Zoom's process/address space, an attacker automatically gains all access rights, including control of the camera and microphone. [7]

A further two 0days affecting Windows and macOS clients were offered for sale on the Darknet. The Windows bug is a remote code execution issue which is, according to an industry expert, "perfect for industrial espionage." It would need to be coupled with another bug, however, to successfully access a target machine. Despite this, several brokers had reportedly offered $500,000 for it. The 0day in macOS is not a remote code execution making it less dangerous for users and harder to use in a real hack. There is little information regarding this issue and the researchers who discovered it provided no further indication of the way in which it functions. [8]

Zoom is not the only video chat application that is being used as a lure in malware campaigns. Threat actors are also exploiting the names of other remote working software to steal credentials and deliver malware, including Cisco WebEx. A notable phishing operation purported to be a Cisco "critical update" from the spoofed address - meetings@webex[.]com. It informed the victim that they need to patch CVE-2016-9223 and included a link to a fake update page. [9] Another campaign used illegitimate copies of Skype to deliver malware. Two adware families were prominent in many of the apps: DealPly and DownloadSponsor. These display aggressive advertisements once the applications are downloaded. Other Skype-themed apps are exploiting a vulnerability designated CVE-2010-2568 to infect victims with additional malware. This flaw uses Windows Shell that is not properly handled during icon displays in Windows Explorer. The bug received a patch several years ago, however, so the exposure landscape is limited. [10]

Undoubtedly, Zoom has become an attractive target for threat actors and pranksters. However, it is worth noting that the majority of exposures are from personal accounts with weak or no passwords. Zoom is taking steps to patch address security concerns, most of which can be mitigated by using a strong and unique password. Despite this, many government departments have discouraged Zoom use for sensitive discussions, including the Ministry of Defence. However, it is worth noting that NCSC guidance indicates that there is no reason for Zoom not to be used for conversations below a certain classification. [11]

5G Disinformation

Disinformation, misinformation and conspiracy theories have become so prevalent, the WHO has declared an "infodemic" and warned of the potential impact on global health. [1] Various unsubstantiated claims about the disease are circulating, including one that is presenting a significant threat to the critical infrastructure sector. According to its adherents, 5G networks are either directly responsible for the coronavirus pandemic or exacerbating its severity and spread. Despite numerous official sources stating that the allegations are false, the rumours have had significant real-world consequences. Across the UK, activists have set fire to what they believed were 5G masts at over 20 locations. [2]

The anti-5G movement gained momentum in 2018 after major mobile networks began trialling the technology. Shortly after, several anti-5G groups emerged on Facebook, including "Stop5GUK", which attracted over 27,000 members. [3] Activist Mark Steele is one of the most prominent anti-5G voices. He has made various claims over the past two years, including that 5G kills babies, causes cancer and is being secretly deployed in lamposts in Gateshead. Despite attempts by Gateshead Council to silence Steele in 2018, a judge ruled that the public had a "right to know" about 5G conspiracy theories. [4] Since then, the anti-5G movement has steadily gained momentum in the UK, spawning various outlandish claims about the potential negative health effects of 5G technology. Unfortunately, this has now escalated into physical attacks on telecommunications equipment, putting our communications infrastructure at risk when it is needed most.


Sal Fadhley shared his first post.
New member • Yesterday at 11:01 •
They have just started installing 5G lamp-posts in the park near where I live. That's why I have stopped going out at night. I spoke with weapons expert Mark Steele who confirmed that they are the exact same model. These are part of the kill grid. Folks, they may look harmless but Steele confirms that they can kill you or blind you.

Fig.9 - 5G conspiracy theorist claims 5G transmitters installed in lamp posts

Our research identified numerous 5G conspiracy theories. Some implied alleged that it was a weapon of a foreign power being used against the British public. Others alleged that it was part of a government strategy to control the future population. On YouTube, some content creators have pushed the theory that China created the technology to amplify the spread of COVID-19. They believe that the virus was manmade and that states with 5G equipment are at greater risk of COVID-19-related fatalities. These theories are supported with dubious comparisons between the death rates of countries with 5G infrastructure and those without. China's ultimate goal, it is alleged, is to achieve global hegemony using 5G and COVID-19.

A common theory among far-right Telegram groups is that 5G is an Israeli weapon. It is alleged that security services Shin Bet and Mossad designed 5G to depopulate the West using radio frequencies that damage reproductive ability. The theory is supported with claims that 5G is banned in Israel to protect fertility, with photoshopped articles provided as evidence.

Fig.10 - Telegram users claims Israel bans 5G technology

Another theory that has gained traction claims that 5G is designed to make the world harder to inhabit. Images and videos of dead animals near 5G infrastructure are used to push this theory. Proponents believe 5G is a government ploy to depopulate working-class communities to reduce the burden on the state. This has spawned a subsequent theory that 5G is intended to depopulate countries to create a globalist world with no borders and a single government. The final theory that has gained support among far-right groups, states that 5G will be deployed in conjunction with IoT devices to increase surveillance on populations.

Fig.11 - Website alleging 5G is used for population control

Our research has confirmed the existence of a substantial 5G conspiracy theory community in the UK. These communities are spread across all major platforms. However, most of the chatter is present on Telegram and Facebook, with video content disseminated on BitChute and YouTube. While some members are opposed to attacking infrastructure, a significant number claim that they are prepared to act against 5G infrastructure in the future.

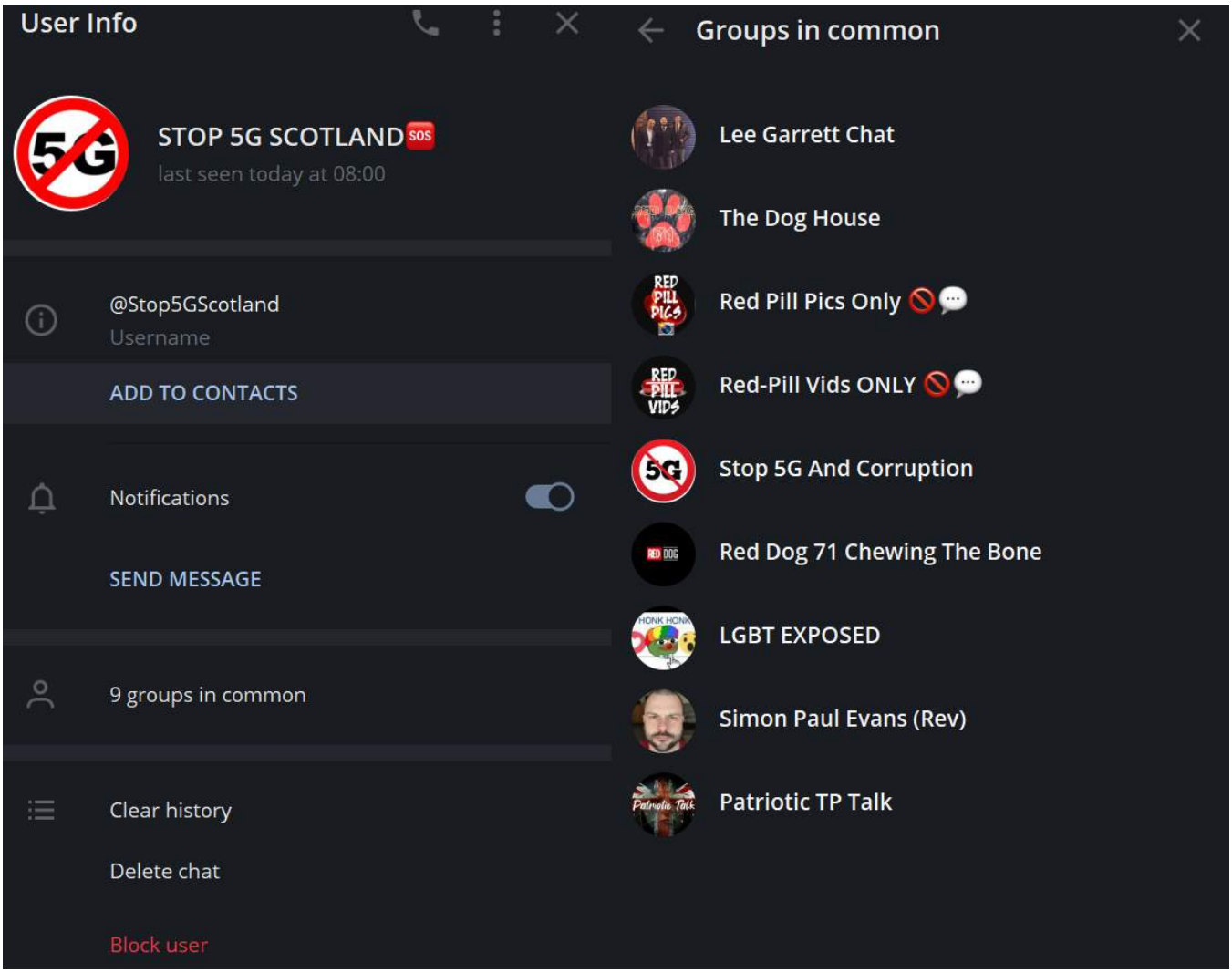

Fig. 12 - Anti-5G Telegram channel linked to far-right groups

Videos like this from Mark Steele are typically shared amongst groups on Telegram. They contain various unfounded claims that are intended to incite attacks on 5G and even 4G infrastructure. These are shared not only on 5G specific chats but also in generic political groups in an attempt to attract new members to the cause. The most prominent conspiracy theory propagated on 5G-specific Telegram chats alleges that 5G is intended to depopulate society, particularly the working class.

Further investigation of 5G conspiracy groups indicated that many members are also members of far-right chats. Indeed, recruitment for 5G groups was mainly undertaken by flooding far-right groups with a variety of 5G conspiracy theories. The convergence of these two communities is seemingly causing an escalation in more extreme approaches to 5G technology. For example, an increasing number of members are suggesting that destroying cell towers is a nationalist duty to protect future generations. Other users, such as those below, have used Telegram to discuss their methods of attack:

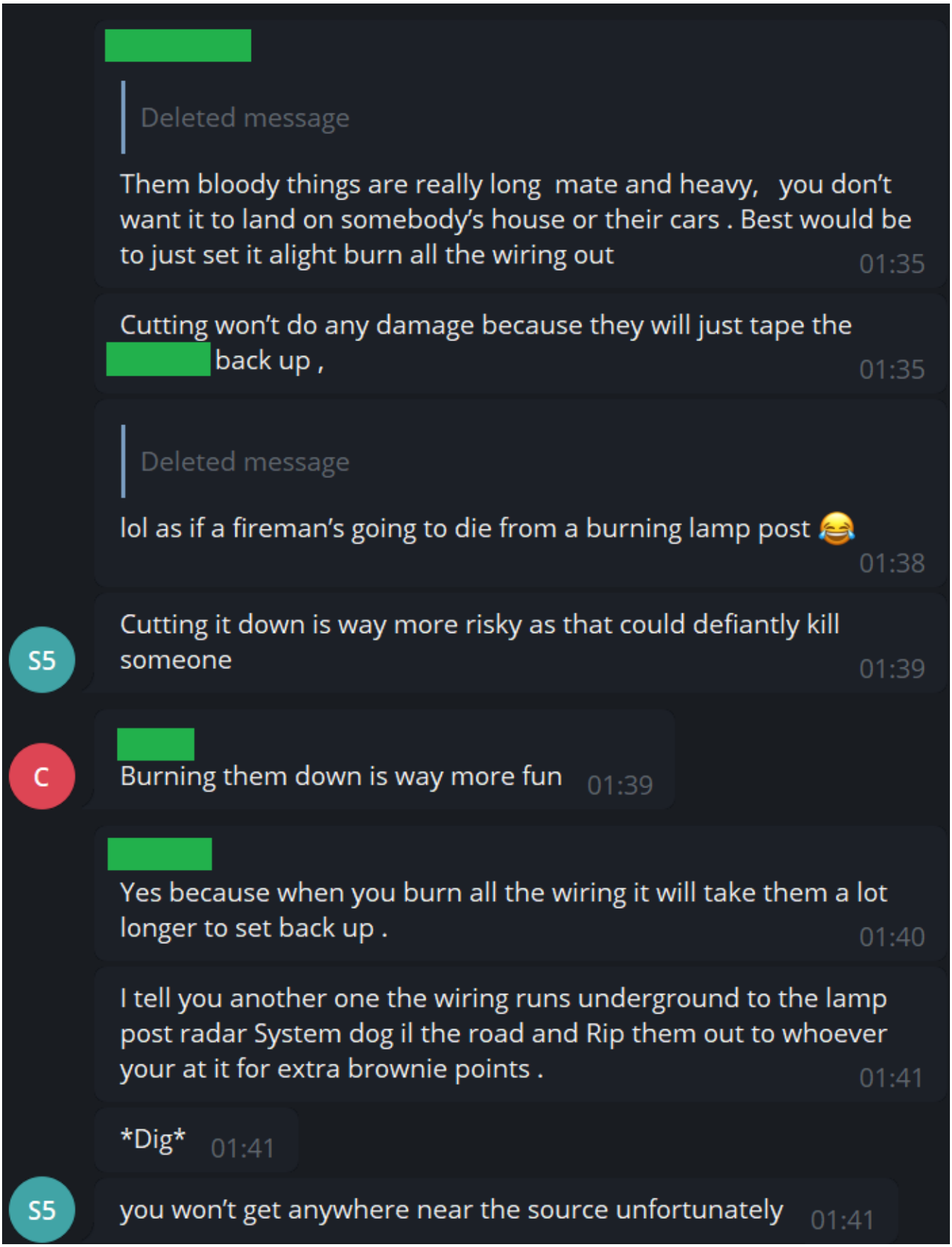

Fig.13 - Users discuss vandalising 5G masts

As expected, anti-5G chatter on Facebook is more prevalent and less secretive. Groups with hundreds of thousands of members could be found easily. Unlike Telegram, the users were more diverse both demographically and in terms of motive. Some group were created solely to monitor the roll-out of 5G in specific areas; others opposed 5G as part of a broader environmentalist strategy. This variety provided greater insights into attitudes towards 5G technology and why it is considered a threat.

In general, members of Facebook groups tended to be less extreme than those on Telegram. However, we did identify some whose members regularly discuss the destruction of 5G infrastructure. Phrases such as “burn it”, “take it down” and “pull it down” are common whenever a user identified a new mast nearby. Proponents of these more extreme approaches tend to treat the destruction of 5G infrastructure as a moral imperative.

Fig.14 - Facebook users threaten to destroy 5G equipment

Cyjax's Social Media Threat Intelligence team can monitor this and any other campaign that presents a threat to critical infrastructure on social media, instant messaging and the darknet. This can provide a strategic overview of the theories underpinning anti-5G conspiracies, alongside more tactical intelligence about the individuals and groups involved. Our dedicated team of SOCMINT analysts is skilled at infiltrating these groups undetected, passively monitoring them and gleaning actionable intelligence that can help protect UK communications infrastructure during the coronavirus pandemic.

Vulnerabilities

This section provides an overview of the vulnerabilities that threat actors are exploiting as part of the coronavirus pandemic, alongside some additional recent high severity vulnerabilities that could impact critical infrastructure.

COVID-19 exploited vulnerabilities

CVE-2017-8570 – Microsoft Office allows a remote code execution vulnerability due to the way that it handles objects in memory, aka "Microsoft Office Remote Code Execution Vulnerability".

A new malware campaign pushing an EternalBlue downloader Trojan has been identified. It is delivered via the recently discovered BlueTea worm. The campaign relies heavily on COVID-19-themed spam emails to infect victim devices.

The BlueTea worm's spam emails' subject is typically "The Truth of COVID-19" and contains a malicious RTF document that exploits CVE-2017-8570.

Once a malicious document is opened, the victim's device is infected with the EternalBlue downloader Trojan. The Trojan is able to load other viruses onto the infected device and can steal credentials, emails addresses from Outlook, and offer remote control of the infected device for the attackers.

CVE-2019-19781 - vulnerability in Citrix Application Delivery Controller and Citrix Gateway leading to arbitrary code execution. The vulnerability has been exploited in numerous high-profile intrusions in recent months, including New York state government and Bretagne Télécom (Brittany Telecom), which was infected with the DoppelPaymer ransomware. In addition, it is being leveraged in Iranian and Chinese cyberespionage operations against multiple countries, including UK critical infrastructure sectors.

CVE-2020-10189 - Zoho ManageEngine Desktop Central before 10.0.474 allows remote code execution because of deserialization of untrusted data in getChartImage in the FileStorage class. Exploitation was identified in the wild in early March, including by Chinese state actor APT41 against multiple countries, including UK critical infrastructure sectors.

CVE-2019-1653, CVE-2019-1652 (Cisco RV320 and RV325) - A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information.

The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information. Cisco has released firmware updates that address this vulnerability.

Both vulnerabilities are being exploited in the wild, including Chinese state actor APT41 against multiple countries, including UK critical infrastructure sectors.

CVE-2019-3396 - The Widget Connector macro in Atlassian Confluence Server before version 6.6.12 (the fixed version for 6.6.x), from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x), allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.

Multiple threat groups are exploiting this vulnerability, including Rocke, a Chinese threat group that hijacks machines to mine cryptocurrency. This is another vulnerability that APT41 is exploiting to install a backdoor on the victim machine and download custom malware.

CVE-2017-11882 - Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11884.

Numerous APT groups have exploited the vulnerability in recent months, including Indian APT SideWinder, PatchWork, SWEED, GroupA21 and ViciousPanda. A broad range of sectors has been targeted, including critical infrastructure. Various malware are being delivered via this vulnerability, including Loda RAT and LokiBot.

CVE-2012-0158 - The (1) ListView, (2) ListView2, (3) TreeView, and (4) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Office 2003 Web Components SP3; SQL Server 2000 SP4, 2005 SP4, and 2008 SP2, SP3, and R2; BizTalk Server 2002 SP1; Commerce Server 2002 SP4, 2007 SP2, and 2009 Gold and R2; Visual FoxPro 8.0 SP1 and 9.0 SP2; and Visual Basic 6.0 Runtime allow remote attackers to execute arbitrary code via a crafted (a) web site, (b) Office document, or (c) .rtf file that triggers "system state" corruption, as exploited in the wild in April 2012, aka "MSCOMCTL.OCX RCE Vulnerability."

A broad range of threat actors are exploiting this vulnerability. Most recently, a coronavirus themed phishing campaign targeted governments and medical organisations worldwide. A ransomware family, dubbed EDA2, has been observed in several attacks on a Canadian government healthcare institution and a Canadian medical research university.

CVE-2010-2568 - Windows Shell in Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7 allows local users or remote attackers to execute arbitrary code via a crafted (1) .LNK or (2) .PIF shortcut file, which is not properly handled during icon display in Windows Explorer, as demonstrated in the wild in July 2010, and originally reported for malware that leverages CVE-2010-2772 in Siemens WinCC SCADA systems.

Several Skype-themed malicious applications have been recently found exploiting the flaw. However, since it was patched several years ago, the number of vulnerable systems is limited.

CVE-2019-9621 - Zimbra Collaboration Suite before 8.6 patch 13, 8.7.x before 8.7.11 patch 10, and 8.8.x before 8.8.10 patch 7 or 8.8.x before 8.8.11 patch 3 allows SSRF via the ProxyServlet component.

CVE-2019-9670 - mailboxd component in Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10 has an XML External Entity injection (XXE) vulnerability.

Both vulnerabilities are being exploited to deliver the Formbook infostealer. Numerous organisations have been targeted, including those operating in the critical infrastructure space.

General ICS vulnerabilities

CVE-2020-6971 - In Emerson ValveLink v12.0.264 to v13.4.118, a vulnerability in the ValveLink software may allow a local, unprivileged, trusted insider to escalate privileges due to insecure configuration parameters.

CVE-2020-8768 - An issue was discovered on Phoenix Contact Emalytics Controller ILC 2050 BI before 1.2.3 and BI-L before 1.2.3 devices. There is an insecure mechanism for read and write access to the configuration of the device. The mechanism can be discovered by examining a link on the website of the device.

CVE-2020-6986 - In all versions of Omron PLC CJ Series, an attacker can send a series of specific data packets within a short period, causing a service error on the PLC Ethernet module, which in turn causes a PLC service denied result.

The previous three vulnerabilities impact ICS products used in chemical, manufacturing, energy, food and agriculture, healthcare, nuclear reactors, materials and waste, transportation systems, and water sectors.

CVE-2019-5073, CVE-2019-5074, CVE-2019-5075, CVE-2019-5077, CVE-2019-5078, CVE-2019-5079, CVE-2019-5080, CVE-2019-5081, CVE-2019-5082 - multiple vulnerabilities have been identified in WAGO ICS products. If successfully exploited, these could lead to unauthorised modifications, deletion of the application, remote code execution, denial of service, revert to factory settings, and overwrite MAC addresses.

The affected products include:

- WAGO I/O-CHECK Series PFC100 (750-81xx/xxx-xxx)
- WAGO I/O-CHECK Series PFC200 (750-82xx/xxx-xxx)
- WAGO I/O-CHECK 750-852, 750-831/xxx-xxx, 750-881, 750-880/xxx-xxx, 750-889
- WAGO I/O-CHECK 750-823, 750-832/xxx-xxx, 750-862, 750-890/xxx-xxx, 750-891

WAGO ICS products are used in commercial facilities, energy, manufacturing, and transportation systems worldwide.

CVE-2019-5107, CVE-2019-5134, CVE-2019-5135, CVE-2019-5149, CVE-2019-5155, CVE-2019-5156, CVE-2019-5157, CVE-2019-5158, CVE-2019-5159, CVE-2019-5160, CVE-2019-5161, CVE-2019-5166, CVE-2019-5167, CVE-2019-5175, CVE-2019-5176, CVE-2019-5182, and CVE-2019-5184 – additional vulnerabilities were discovered in WAGO's e! COCKPIT automation software. If exploited, these could lead to command injection, information disclosure, or remote code execution.

CVE-2020-6990, CVE-2020-6984, CVE-2020-6988, CVE-2020-6980 - Multiple critical vulnerabilities have been found in industrial control system (ICS) equipment from Rockwell Automation and Johnson Controls. The bugs impact programmable logic controllers (PLC) and physical access control systems, which control physical machines in facilities.

CVE-2020-6990, can allow an attacker to find a cryptographic key and use it for further cryptographic attacks. These attacks could lead to a remote attacker gaining full, unauthorised control of the machine controller. This bug is caused by the cryptographic key being used to protect the hard-coded account password stored in the binary file. The actual cryptographic function used to protect the password is also discoverable (CVE-2020-6984).

Another vulnerability, an authentication bug tracked as CVE-2020-6988, can allow a remote and unauthenticated attacker to send a request from the RSLogix 500 software to the victim's MicroLogix controller. The request causes the controller to send back used password values for authentication. This facilitates authentication bypass, sensitive information disclosure, and credential leakage.

A fourth bug was also found in the email function. This flaw is tracked as CVE-2020-6980, and is a cleartext storage vulnerability. If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, an attack with access to a victim's project could gather any data written in cleartext.

An improper input validation bug, tracked as CVE-2019-7589, was also found in the Johnson Controls' Kantech EntraPass product. This flaw could allow an attacker to execute malicious code with system-level privileges, and give the attacker the ability to chose who is allowed to access the facilities.

To mitigate the chances of attack, users of MicroLogix 1400 series B controllers and RSLogix 500 software should update to the latest version. There are, however, no mitigations for MicroLogix 1400 series A controllers or MicroLogix 1100 controllers. Several other low-level flaws were also disclosed.

CVE-2019-6568, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-10936, CVE-2019-10923, CVE-2019-10929, CVE-2019-10943, CVE-2019-19281, CVE-2019-19282, CVE-2019-13940, CVE-2019-13946, CVE-2020-7579, CVE-2019-19290, CVE-2019-19291, CVE-2019-19292, CVE-2019-19293, CVE-2019-19294, CVE-2019-19295, CVE-2019-19296, CVE-2019-19297, CVE-2019-19298, and CVE-2019-19299

Multiple vulnerabilities have been disclosed for Siemens ICS products, including:

- Siemens SiNVR 3
- Siemens Spectrum Power 5
- Siemens PROFINET-IO Stack (Update A)
- Siemens SIMATIC S7 (Update A)
- Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update A)
- Siemens SIMATIC S7-1500 (Update A)
- Siemens SPPA-T3000 (Update A)
- Siemens SIMATIC Products (Update B)
- Siemens SIMATIC S7-1200 and S7-1500 CPU Families (Update A)
- Siemens Industrial Real-Time (IRT) Devices (Update C)
- Siemens PROFINET Devices (Update D)
- Siemens Industrial Products (Update E)
- Siemens Industrial Products with OPC UA (Update F)
- Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update G)
- Siemens S7-300/400 PLC Vulnerabilities (Update E)

CVE-2019-18998, CVE-2019-19000, CVE-2019-19001, CVE-2019-19002, CVE-2019-19003, CVE-2019-19089, CVE-2019-19090, CVE-2019-19091, CVE-2019-19092, CVE-2019-19093, CVE-2019-19094, CVE-2019-19095, CVE-2019-19096, and CVE-2019-19097

Multiple vulnerabilities have been identified in ABB ICS products in the energy sector. The products affected include:

- ABB eSOMS 6.02 and prior
- ABB Asset Suite Versions 9.6 and prior, excluding 9.4.2.6 and 9.5.3.2

Successful exploitation can lead to taking over of a user's browsing session, the discovery of session-based information, or affect the confidentiality of sensitive information within the application.

CVE-2020-7478, CVE-2020-7479 – A security advisory was released for multiple vulnerabilities in Schneider Electric SCADA software deployed in ICS environments in commercial facilities, manufacturing, and energy facilities. Successful exploitation of these vulnerabilities could result in unauthorised access to sensitive data and functions.

The products affected include:

- Schneider Electric IGSS SCADA Software, versions 14 and prior using the service IGSSupdate
- Schneider Electric has provided IGSS14 Version 14.0.0.20009 to address these vulnerabilities.

CVE-2020-6994 - A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. Hirschmann recommends updating HiOS products to Version 07.0.03 or higher, and HiSecOS products to Version 03.3.00 or higher.

CVE-2019-6857, CVE-2019-6856, CVE-2018-7794, CVE-2019-19100, CVE-2019-19101, CVE-2019-19102 – multiples vulnerabilities have been disclosed in Schneider Electric ICS products. Successful exploitation could result in a denial of service attack. The industries affected include energy, manufacturing, and other commercial facilities.

For CVE-2019-6857, the following Modicon PLC are affected:

- Modicon M580, all versions prior to v2.80
- Modicon M340, all versions prior to v3.01
- Modicon Premium, all versions prior to v3.20
- Modicon Quantum, all versions prior to v3.60

For CVE-2019-6856 and CVE-2018-7794, the following Modicon PLC are affected:

- Modicon M580, all versions prior to v2.80
- Modicon M340, all versions prior to v3.01
- Modicon Premium, all versions prior to v3.20
- Modicon Quantum, all versions prior to v3.52

Schneider Electric has developed the appropriate mitigations, specific to Modicon M580 firmware v3.10.

CVE-2019-19100, CVE-2019-19101, CVE-2019-19102 – A security advisory has been issued for vulnerabilities in B&R industrial control systems (ICS). Successful exploitation can lead to the deletion of arbitrary files from the system, fetching of arbitrary files, or performing arbitrary write operations. The industries impacted include chemical manufacturers, critical infrastructure, and energy.

The products affected include:

- B&R Automation Studio, Versions 4.0.x
- B&R Automation Studio, Versions 4.1.x
- B&R Automation Studio, Versions 4.2.x
- B&R Automation Studio, versions prior to 4.3.11SP

- B&R Automation Studio, versions prior to 4.4.9SP
- B&R Automation Studio, versions prior to 4.5.4SP
- B&R Automation Studio, versions prior to 4.6.3SP
- B&R Automation Studio, versions prior to 4.7.2
- B&R Automation Studio, versions prior to 4.8.1

B&R recommends applying product updates at the earliest convenience. Users of Automation Studio Versions 4.0.x, 4.1.x, and 4.2.x are advised to upgrade to a newer version of Automation Studio.

CVE-2020-10621, CVE-2020-10617, CVE-2020-10623, CVE-2020-10619, CVE-2020-10631, CVE-2020-10625, CVE-2020-10629, CVE-2020-10603, CVE-2020-6992, CVE-2020-10633, CVE-2020-10646, CVE-2020-10635, CVE-2019-20046, CVE-2019-20045, CVE-2019-16879, CVE-2020-7800, CVE-2020-7801, CVE-2020-7802 – Multiple vulnerabilities have been discovered in ICS, SCADA, and PLC products.

The products affected include:

- Advantech WebAccess/NMS (ICSA-20-098-01)
- GE Digital CIMPLICITY (ICSA-20-098-02)
- HMS Networks eWON Flexy and Cosy (ICSA-20-098-03)
- Fuji Electric V-Server Lite (ICSA-20-098-04)
- KUKA.Sim Pro (ICSA-20-098-05)
- Synergy Systems & Solutions HUSKY RTU (ICSA-20-042-01)

CVE-2020-7574, CVE-2020-7575, CVE-2018-5390, CVE-2018-5391, CVE-2019-13940, CVE-2019-10934 - multiple security warnings have been disclosed for vulnerabilities in Siemens industrial control systems. The most critical vulnerabilities can lead to remote code execution, remote denial of service, and the ability to locally execute code with system privileges. Manufacturing, water management, energy, and critical infrastructure sectors are affected.

The products affected include:

- Siemens Climatix POL908 (BACnet/IP module) and POL909 (AWM module); all versions. (ICSA-20-105-04)
- Siemens IE/PB-Link, RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (ISCA-20-105-05)
- Siemens SIMATIC S7 (ISCA-20-042-05)
- Siemens TIA Portal (ISCA-20-014-05)

A vulnerability has been discovered in some Field Programmable Gate Array (FPGA) chips which can expose devices to attacks. These chips are present in a wide range of systems including industrial control systems (ICS), cloud data centres, cellular base stations, medical devices, and aviation systems. This flaw has been given the name Starbleed.

The flaw can be exploited by attackers to take full control of an FPGA chip. In order to exploit the flaw, an attacker would need to have access to a device's JTAG or SelectMAP interfaces. Researchers have warned, however, that remote attacks could also be possible. If control of the chip is achieved, attackers can plant hardware backdoors, change the device's functionality, or cause physical damage to the system. (source)

Advice

- Ensure antivirus software is kept up to date.

- Do not open files or links from sources that you do not know.
- Ensure Zoom meetings are password-protected.
- 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.
- Ensure all critical systems are patched, particularly when known vulnerabilities are being exploited in the wild.
- 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.
- Monitor 5G conspiracy theories to identify credible threats.
- Only purchase masks, hand sanitiser and related products from reputable stores.

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