COVID-19 & Cyber Threats

MARCH 2020

Cyberint

TABLE OF CONTENTS

Table of Contents 2

Executive Summary 3

COVID-19: Business & Cyber Disruption 4

Cyberint Research Insights 4

- Remote Working 4
- Malicious Campaigns 5
- Ransomware 7
- Disinformation/Fake News 7
- Fraud 8

Cyberint Recommendations 10

Contact Us 12

EXECUTIVE SUMMARY

As the ongoing COVID-19 (Coronavirus) pandemic spreads around the world, the unprecedented and evolving global situation has created numerous opportunities for threat actors to leverage the worldwide concern and anxiety in their nefarious campaigns.

Utilizing thematic lures, a variety of cyberattacks have been launched during a time when many are seeking critical information on the outbreak. Exploiting the headline-dominating crisis, individuals, organizations and governments alike are tricked into opening malicious payloads, visiting malicious websites and are subject to misinformation or fraud. Increased remote working patterns, especially for those not accustomed, can lead to increased cyberthreat exposure.

Key Findings

- Cybercriminals and nation-state threat actors are exploiting COVID-19 via thematic lures leading to malicious payloads and links,
- Off-the-shelf attack kits mimicking a COVID-19 case map available for sale on the deep/dark web,
- Ransomware threats continue with a health authority becoming victim,
- Potentially fraudulent sales of hard-to-obtain products exploiting the global situation,
- Fake news and misinformation is used to potentially cause panic and civil unrest in specific regions

Cyberint Recommendations

- Raise employees' pandemic situational awareness
- Raise employees' cybersecurity situational awareness with specific known campaigns
- Assess and update your cybersecurity policy to address scale of remote workers
- Practice good cybersecurity hygiene, and communications
- Ensure you have full visibility of verified threats; have zero tolerance to non-relevant alerts
- *Now more than ever* – Act on intelligence to reduce dwell time and impact on your business continuity

COVID-19: BUSINESS & CYBER DISRUPTION

COVID-19 has already caused, and will continue to cause, disruption to business operations and continuity worldwide. As we all adapt and change the ways in which we work, shop, travel and interact with various services, these changes will likely stay in effect for months or years - to come – if not forever. These changes bring new cyber challenges.

Dramatic changes in customer demand and behavior are putting organizations under stress: aside from the need to maintain continuity of service and protecting both customers and employees, supporting security business operations will be at the forefront of many executives' minds to prevent disruptions and avoid financial challenges. Those that are ill-prepared, in the face of demand surges and resource shortages eventually risk disengaging customers with any service failures or shortcomings.

Combined with exponential growth in cloud, web and mobile applications and digital-based collaboration, this global pandemic serves as an unfortunate ideal foundation to create a cybersecurity perfect storm.

With many organizations being faced with the impacts of COVID-19, such as a reduced workforce and the need to support remote working at scale, either voluntary or in response to government movement restrictions, this report seeks to summarize the nature of the attacks observed thus far to allow organizations to be better prepared in protecting themselves and their employees, in addition to families and friends, in the coming weeks and months.

CYBERINT RESEARCH INSIGHTS

REMOTE WORKING

Whilst many organizations already have robust remote working policies and procedures, government restrictions on movements combined with an organization's duty of care to their employees has seen an unprecedented jump in those working from home.

Aside from logistical needs, remote workers bring a unique set of security challenges along with the need for system capacity and availability that can cope with increasing numbers of remote users.

Typically, employees working within an organization's infrastructure will be protected by various security controls be that implemented on the devices in front of them on their desks all the way through to the organization's network perimeter. Whilst end-point security controls may remain operational when desktop machines or laptops are taken home for 'remote working', connecting to unmanaged home networks may increase the exposure and risk for end-users, especially as many may not maintain high-levels of security discipline outside of the workplace.

Given the observed use of COVID-19 thematic lures, and the likely absence of security controls across home networks that would prevent access to suspicious or malicious websites, remote employees are particularly susceptible to campaigns that feed upon the current uncertainty, especially as people seek and crave more information on the crisis.

Furthermore, working within the home environment may cause many to forget or ignore good cyber security practice and as such, many may be tempted to install vulnerable or untrustworthy software, perhaps to facilitate communications with colleagues or to obtain news, or forget to secure one's data and access when leaving their desks. Such behavior exposes the data to curious eyes or inadvertent change caused by an errant child's finger or curious cat's paw!

MALICIOUS CAMPAIGNS

Thematic lures based on COVID-19 topics allow both broad indiscriminate campaigns to be launched as well as targeted attacks against specific individuals or organizations.

Numerous phishing campaigns have already been observed[1] as masquerading as health agencies including the 'World Health Organization' (WHO) and the United States 'Centers for Disease Control and Prevention' (CDC). These campaigns appear to vary in sophistication, suggesting the tactic is being used by both advanced threat actors and opportunists, and include subject lines that relate to preparedness, outbreaks or even cures (Figure 1).

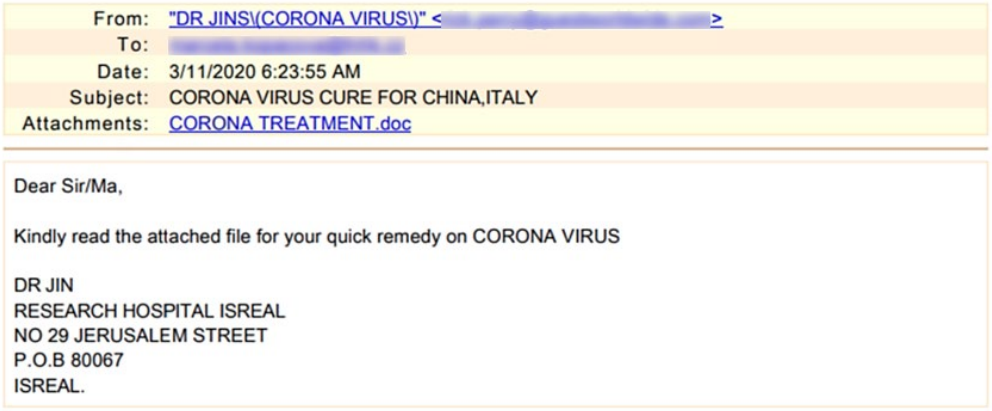

Figure 1 – Example malicious email campaign

Of the campaigns observed thus far, suspected nation-state activity saw the delivery of fake WHO documents being sent to the Ukrainian Ministry of Health, reportedly dropping keylogging malware. Furthermore, similar lures have been received by organizations across Southeast and Central Asia along with Eastern Europe in attacks that would be consistent with a nation-state threat actor engaged in espionage.

It is reported[2] that the Iranian government was responsible for the distribution of a fake mobile application named 'AC19', claiming to determine if the user was infected with the coronavirus, to some

[1] https://www.bloomberg.com/news/articles/2020-03-12/hackers-posing-as-cdc-who-using-coronavirus-in-phishing-attacks

[2] https://www.vice.com/en_us/article/epgkmz/iran-launched-an-app-that-claimed-to-diagnose-coronavirus-instead-it-collected-location-data-on-millions-of-people

3.5 million Iranian citizens via the 'Café Bazaar' mobile app store. The app, in addition to asking questions related to the user's health, reportedly allows real-time location tracking. The motivation behind this activity is not clear, however, Iran has a history of conducting surveillance operations albeit typically against dissidents.

Cybercriminals are using similar lures as well as masquerading as organizational emails that encourage employees to open 'policy' attachments, which are weaponized documents that deliver various malicious payloads. In addition to many threat actors crafting their own COVID-19 themed campaigns, would-be attackers can purchase access to a kit that mimics the popular 'Johns Hopkins University' case tracking map to exploit unsuspecting victims. Selling on underground forums for just $200 (or $700 - with a code signing certificate), the kit claims that it can infected 10,000 visitors daily although this would likely be dependent on the threat actor deploying it to a convincing domain and encourage high-volumes of visitors.

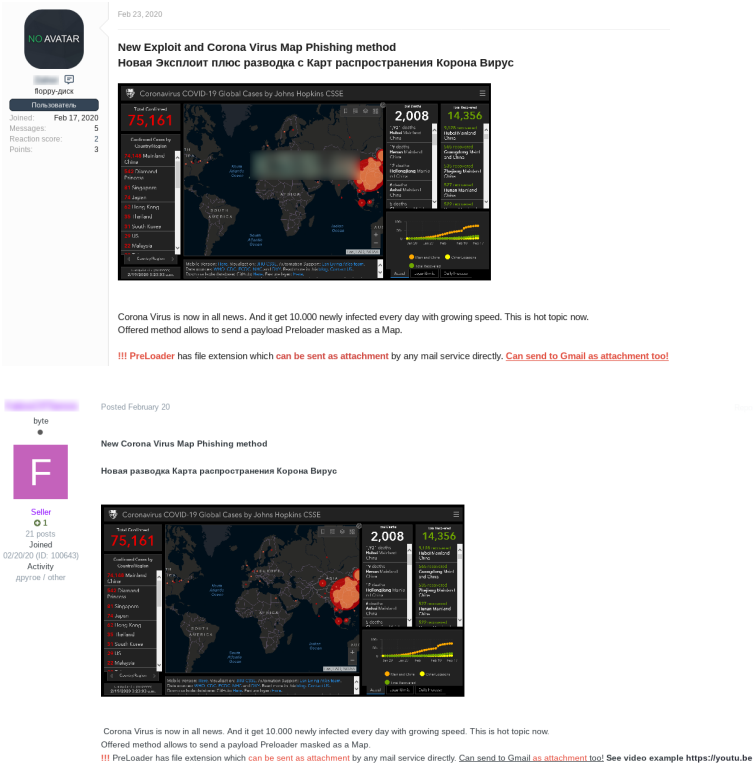

Figure 2 – 'Corona Virus Map' exploit/phishing kit

As more and more businesses seek to inform and reassure their customers, especially those in the hospitality, travel and retail industries, end-users will become accustomed to receiving emails related to the ongoing situation. Somewhat mimicking the transmission of the biological virus, these convincing-looking COVID-19 campaigns can then easily be passed from person-to-person, albeit via unwitting victims sharing nefarious links on social media and messaging groups. As such, users should be reminded to exercise caution when opening any unsolicited email containing links or attachments as well as validating any information given via official government and health authorities.

Undoubtedly, campaigns using COVID-19 as a theme will be prevalent for as long as the virus continues to pose a threat to global health and, as seen in the Iranian-government mobile app 'tracking' campaign, this can lead to huge numbers of victims being lured into opening and executing content unless they are equipped with the knowledge to better protect themselves.

RANSOMWARE

With targeted ransomware attacks being prevalent thus far in 2020, especially those conducted by sophisticated threat actors performing 'steal, encrypt and leak' attacks such as Maze and REvil, a US public health department in Illinois[3] was recently targeted and could see its systems being offline for up to two weeks.

Taking advantage also of individual's seeking information, fake Android applications purporting to be COVID-19 'trackers' have also been observed4 and have resulted in the delivery of 'CoidLock', a mobile ransomware or device locker threat that demands $100 in Bitcoin to unlock the affected device.

DISINFORMATION/FAKE NEWS

In times such as these, where many seek to gain up-to-the-minute information on the outbreak, many will turn to social media and consider what they see as factual truths.

Aside from scaremongering and rumors which can lead to civil unrest, as reportedly[5] occurring in a Ukrainian town following posts that positive COVID-19 victims were to be housed locally, nefarious parties can easily manipulate public opinion and damage brand reputation through spreading lies or misinformation. For example, posts claiming that an individual that has tested positive for the virus has visited a business would dissuade others from visiting and likely spark a costly response as that business takes steps to close and deep clean.

Whilst information remains limited, it is reported[6] that the US Health & Human Services Department was subject to a cyberattack on the 15 March 2020 and subsequently text messages or other communications were circulated to suggest that the US was under national quarantine. Whilst those responsible have not been identified, it is suggested that a 'hostile foreign actor' was responsible for a denial-of-service attack and subsequent disinformation campaign likely in an attempt to cause panic within the United States.

In addition to coordinated disinformation campaigns, a surge in the registration of domains related to COVID-19 have been observed with some 30,000 domains containing the keywords 'corona' or 'covid' being registered since 1 January 2020. Average some 1,300 domain registrations per day so far in March 2020, whilst some may be used for legitimate purposes, keyword registrations based on common topics are often used by those looking to capitalize on increased web traffic, such as to generate advertising revenue, as well as threat actors seeking to add the appearance of legitimacy to their nefarious content.

Many of these domains exhibit behaviors consistent with nefarious activity, such as the use of domain registration services that have less-stringent registrant verification processes or accept payment

[3] https://www.motherjones.com/politics/2020/03/illinois-ransomware-coronavirus/
[4] https://thenextweb.com/security/2020/03/13/hackers-are-spreading-fake-android-coronavirus-trackers-to-steal-your-bitcoin/
[5] https://www.bbc.co.uk/news/world-europe-51581805
[6] https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-9-response

using cryptocurrency, as well as domains that share registrant details or resolve to hosts that are associated with known malicious domains.

Notably, the registration of puny-code domains has also been observed which, in addition to allowing internationalized domains names based on the COVID-19 theme, can be abused to allow the substitution of visually similar characters that can confuse or trick visitors. One such example (Figure 3), mimicking the domain 'coronavirus[.] com', leads to a search redirection domain that has been associated with malicious trojan payloads.

Figure 3 – Example puny-code domain

Notably, the mimicked domain in the above example currently redirects to the official WHO website although does not appear to be owned by them. Previously this domain was 'parked' and displayed advertising content, as such, it should also be considered low reputation.

Given the threats from thematic keyword domains, organizations should be cautious of any newly registered or low-reputation domain related to this topic and ensure that only officially recognized information outlets are visited.

FRAUD

Fraudulent advertisements, products sales and websites have sprung-up to entice would-be victims in to paying for goods or services that may be non-existent, or perhaps more concerningly, substandard or downright dangerous.

For example, underground marketplaces have listings for medical 'N95' masks (Figure 4) that, as normal stocks are depleted, may encourage desperate people to purchase them. Aside from not knowing if the product actually exists, and isn't just a money-making ruse, the product could easily be counterfeit and therefore ineffective at protecting the user.

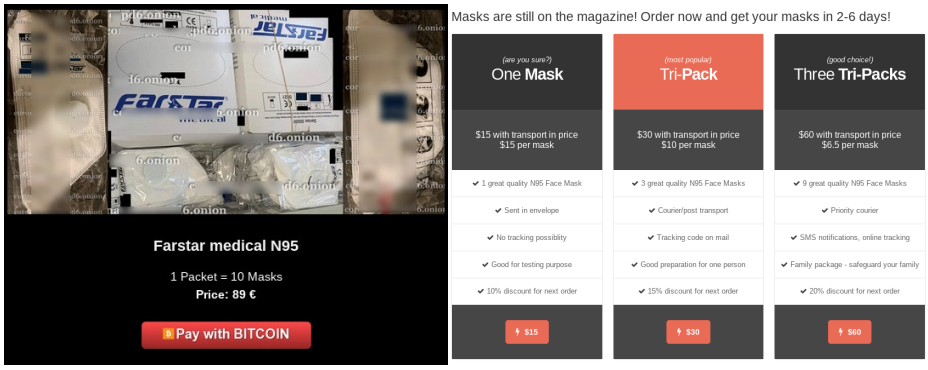

Figure 4 – Underground sales of medical masks

In addition to this occurring on the 'dark web', which is obviously somewhat less traveled by non-technical users, social media posts offering exhausted supplies (Figure 5) are prevalent and may also

be fraudulent. With panic-buying stripping the shelves of many retailers, many individuals or even organizations, may be tempted to source items from alternative suppliers and should therefore exercise caution when dealing with previously unknown sellers.

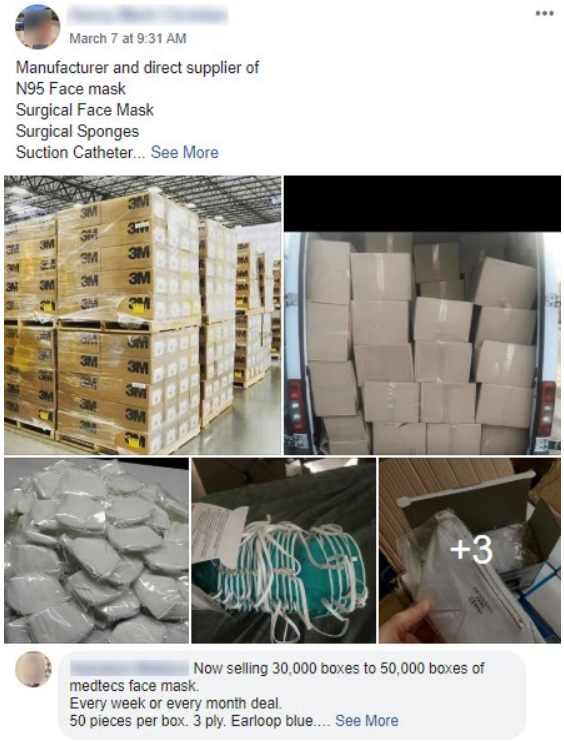

Figure 5 – Potentially illegitimate product sales via social media

CYBERINT RECOMMENDATIONS

RAISE EMPLOYEES' PANDEMIC AND CYBERSECURITY SITUATIONAL AWARENESS

Given the high potential for both misinformation and nefarious websites seeking to capitalize on this situation, those seeking medical or official advice should always refer to recognized sources such as the World Health Organization (WHO)[7] and/or regional government websites.

Generally speaking, employees should be advised to exercise extreme caution in handling any emails with a COVID-19-related subject, attachment, or hyperlinks, just as to be wary of social media, texts, or unsolicited calls related to this issue. Furthermore, organizations should be suspicious of any domains, especially those that are newly registered and with low reputation, that include keywords related to COVID-19 and Coronavirus as threat actors will often try to capitalize on themes and misspellings of legitimate websites to host threats and exploit misdirected visitors.

ASSESS AND UPDATE YOUR CYBERSECURITY POLICY TO ADDRESS SCALE OF REMOTE WORKERS

Strong security policies may already exist, but it is important to review them and ensure they are adequate as your organization transitions to having more people working from home than in an office. It is also important to address the increase and challenges of the shadow IT and cloud technology-based solutions and services in use.

ENSURE YOU HAVE FULL VISIBILITY OF VERIFIED THREATS; HAVE ZERO TOLERANCE TO NON-RELEVANT ALERTS

With employees potentially using more personal devices as they work from home, may lead to poor cybersecurity hygiene. Employees working from home can result in an organization losing visibility over devices, expanding the amount of potential entry points for threat actors through misconfigurations, outdated or unpatched software and more.

PRACTICE GOOD CYBERSECURITY HYGIENE, AND COMMUNICATIONS

Cybersecurity hygiene doesn't stop when you leave the office, employees should be reminded to adhere to security policies, procedures and practices both in and out of their common workplace. Additionally, employees should be reminded of the need to protect corporate data, particularly as it becomes more difficult for organizations to control who has access to what and where it is being stored. Whilst employees undoubtedly trust their families and housemates, data should still be accessed in an appropriate and secure manner, as well as being secured when unattended.

Furthermore, whilst organizations should ensure that employees can work effectively, the installation of unsanctioned or unapproved software should be discouraged, especially as many may seek to install messaging applications or apps claiming to provide COVID-19 information. Threat actors will capitalize on this situation and undoubtedly target applications of this nature, either to exploitation application vulnerabilities, or to distribute weaponized versions. As is the norm, applications installed

[7] https://www.who.int/

on corporate assets should likely be assessed and approved by IT and security teams to ensure that these do not introduce vulnerabilities or expose employees and corporate data to unnecessary risk..

NOW MORE THAN EVER - ACT ON INTELLIGENCE TO REDUCE DWELL TIME AND IMPACT ON YOUR BUSINESS CONTINUITY

In addition to staying informed on public health and safety issues, organizations should keep abreast of cyber threats to ensure that any developments are understood. Whilst the theme may have changed, most threat actors continue to utilize the same tried and tested tactics, techniques and procedures (TTP) in their campaigns. That being said, whilst TTP such as phishing emails and document lures may continue, threat actors will attempt to shift to targeting individuals that may be working remotely rather than attempting to compromise an organization's infrastructure directly..

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City