Cyber Threats Focusing On Covid-19 Outbreak

N Veerasamy
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
nveerasamy@csir.co.za

Abstract: The outbreak of the novel corona virus or Covid-19 has sparked a wave of changes. Social-distancing and remote working meant that increasingly employees and individuals were reliant on Information Communication Technologies (ICT) to connect and gain access to information. In light of the outbreak of the virus, a vast number of users were required to carry out business activities remotely. Users turned to cyberspace for communication, entertainment and information. A critical dependency for ICT emerged. This also resulted in various fraudsters, attackers and criminals seeking to take advantage of the unsettling situation. This paper takes a look at pertinent cyber threats that aimed to utilise the corona virus in order to exploit users. This work aims to show how the health crisis was manipulated for fraudulent cyber schemes, attacks and exploits, as well to create awareness on these cyber threats in order to prevent users from falling victim to them. Furthermore, the paper also looks at the approach of these attacks to identify the main characteristics for the attack execution. This can help with identification and deterrence of Covid-19 related cyberattacks.

Keywords: cyber, corona virus, Covid-19, threat

1. Introduction

Late 2019 saw the outbreak of the novel corona virus named Covid-19. The respiratory ailment is passed from person-to-person and started spreading epidemically in early 2020. It is reported that in late 2019 someone at the Huanan seafood market in Wuhan was infected with a virus from an animal (Readfearn 2020). Scientists say it is highly likely that the virus came from bats but first passed through an intermediary animal in the same way that another coronavirus – the 2002 SARS outbreak – moved from horseshoe bats to cat-like civets before infecting humans (Readfearn 2020). Following the initial infections, the virus began to spread at an epidemic rate. This resulted in various measures to try to curb the spread of the infectious disease.

The world had to learn to operate differently- education, business and collaboration shifted to the digital environment. Social distancing practices meant employees were discouraged from physically going in to the office. Many employees tried to work remotely where possible. Digital technology has played a significant role in the global footprint of communication and accessibility to information. However, the outbreak of Covid-19 heightened the need for this critical dependency. In this time of the pandemic, the usefulness and criticality of information is paramount- from the sourcing of news, statistics, health guidance and governmental announcements, to supporting work operations. ICT plays a pivotal role in sustaining information flows and continued communication capabilities.

The public at large was obligated to stay at home in order to prevent spread of the disease. Physical offices were shut down and many were able to carry out their work remotely while others used the Internet, social media, streaming services and various other online channels in order to entertain or communicate. Schools were also shut down which resulted in various children taking lessons online. Overall, there was an increased requirement for online capabilities in order to support work and learning obligations. However, not all cyber users may be aware of the cyber threats that emerged from the crisis. Cyber criminals are keen to prey on the latest advantage point and Covid-9 provided a prime opportunity for cyber scams and schemes. "These scams include impersonating government organizations like the World Health Organization to try to solicit donations or trick users into downloading malware; pretending to have information about government stimulus payments; and phishing attempts aimed at workers who are working remotely (Lyons 2020)".

In the uncertain times surrounding the virus, cyber attackers wanted to hone into people's fear and confusion by tricking them into installing malicious software, spreading misinformation or stealing their sensitive data and money.

This paper looks at the cyber threats that arose after the breakout of the corona virus that aimed to use the health pandemic as a bait to exploit users. It aims to show the exploitation of cyber attackers, as well as create awareness of how to curb cyber threats that emerge from the trending conditions.

2. Threat Discussion

In these unsure conditions, many users are required to carry out business and work operations from home. In addition, the public has a strong need to remain abreast of breaking and emerging news stories, as well as health guidance. This intensified users' engagement with news agencies, communications platforms including social media. In an effort to get the latest news story or connect with a third party, users may put themselves at risk. This section looks at the prevalent cyber threats that emerge from the Covid-9 health crisis. A discussion follows on each of the modus operandi of these threats.

The main approach of the cyber threats can be seen as stemming from social engineering. Social engineering is a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites (Kapersky 2020). Criminals try to prey on users' lack of knowledge and convince them to click on links or disclose personal information. Users may be unaware of how their sensitive data can be manipulated. Urgency, fear, authority or intrigue are techniques used to convince users to carry out actions that actually disclose personal information or infect themselves. The emotional aspect of the interaction distracts people and serves to interfere with the potential victim's ability to carefully analyse the content of the message (Workman 2007). Social engineering attacks are often carried out by calling a user and impersonating a person of authority from the bank, lawyer or retail company. However, in the Covid-9 con-text, users may be targeted on social media, or through phishing emails or SMS. Amidst the stressful unfolding of Covid-19, users may receive messages or links pertaining to the health crisis and in an effort to remain up-to-date may click on these messages and links in order to access the latest information.

Semantic attacks are the specific type of social engineering attacks that bypass technical defences by actively manipulating object characteristics, such as platform or system applications, to deceive rather than directly attack the user (Heartfield and Loukas 2015). Commonly observed examples include obfuscated URLs, phishing emails, drive-by downloads, spoofed websites and scareware to name a few (Heartfield and Loukas 2015).

According to Bisson (2019) some of the techniques used to carry out social engineering attacks include:

- **Phishing:** attempts to trick users to disclose personal information like names, email addresses, login credentials, passwords and identity numbers. Users may be sent embedded links that actually redirect users to malicious sites that capture users' data. A sense of urgency is used to manipulate users to act against their better judgement. Examples include corona related news sites or medical status checks.
- **Pretexting:** Through the use of a fabrication scenario, users are convinced into confirming or disclosing personal information. This type of attack requires the attacker to create a realistic story. The story often portrays a sense of fear of urgency while developing a relationship and a level of trust with the victim. For example, users could be relayed a message that someone they were recently in physical contact with, has been infected with Covid-19. Users are urged into disclosing sensitive information in order to check medical status and get health updates.
- **Baiting**: similar to phishing attacks, baiting entices the user with lure of promised goods or items if login credentials are supplied. This type of attack often make use of digital on-line schemes and can be initiated through the use of physical media. For example, users are tricked into purchasing fake goods like hand santizer, masks, gloves or other Personal Protective Equipment (PPE). In an effort to purchase these sought after items, users may disclose banking or credit card credentials.
- **Quie pro quo**: this type of attack is similar to Baiting but is offered as urgent technical services that the user requires. Attackers often impersonate IT, hardware or software representatives and pretend to provide technical assistance to users. Users are convinced of their authenticity but the attacker is aiming to infect users with malware or gather information. Example, users might be sent messages/links or claims that their software is out of date and in order to remain up-to-date about the latest Corona updates, they will need to update software. Users are instructed to disclose login information in order to execute updates.

These examples are indicative of how users can be tricked into social engineering attacks. In the next section, additional semantic examples are discussed in order to demonstrate the use of the corona virus as bait to carry out cyber exploits.

3. Threat Examples

Figure 1 shows a summary of the main examples of semantic threats that can be used to exploit the Covid-19 virus. Fig 1 shows different attack families and example exploits (Adapted from Heartfield and Loukas 2015).

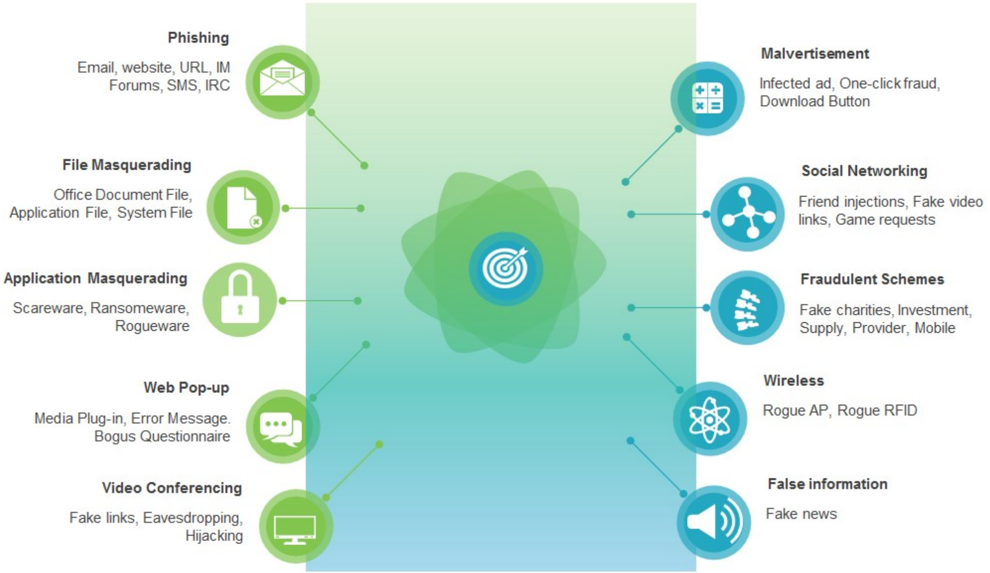

Phishing
Email, website, URL, IM Forums, SMS, IRC
File Masquerading
Office Document File, Application File, System File
Application Masquerading
Scareware, Ransomeware, Rogueware
Web Pop-up
Media Plug-in, Error Message. Bogus Questionnaire
Video Conferencing
Fake links, Eavesdropping, Hijacking
Malvertisement
Infected ad, One-click fraud, Download Button
Social Networking
Friend injections, Fake video links, Game requests
Fraudulent Schemes
Fake charities, Investment, Supply, Provider, Mobile
Wireless
Rogue AP, Rogue RFID
False information
Fake news

Figure 1: Semantic Attack Examples

In the next sections, examples of the exploits are discussed in more detail in order to show users how they are exploited based on the Covid-19 virus.

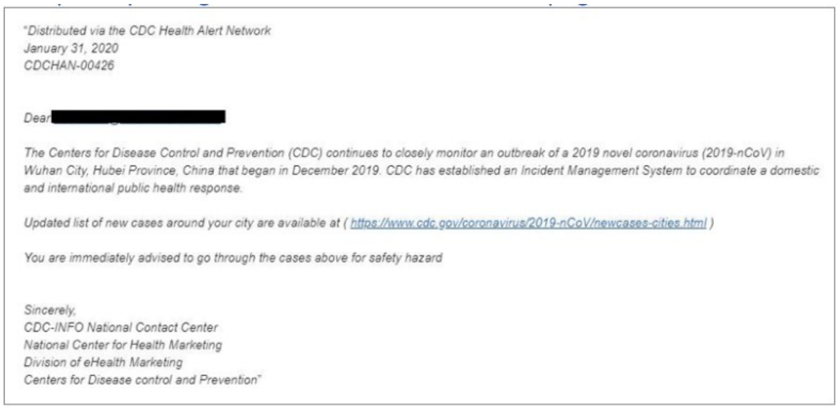
3.1 Phishing

“Hackers and cyber scammers are taking advantage of the coronavirus disease (COVID-19) pandemic by sending fraudulent email and WhatsApp messages that attempt to trick you into clicking on malicious links or opening attachments “ (WHO 2020).

Phishing emails appear to come from legitimate sources like news agencies, the government and companies like banks, retail sector, insurance or health authorities. However, users are tricked into clicking on links or inserting personal information. Malicious websites may be disguised to present important information about the pandemic. Hackers may be developing malicious websites that actually infect users with malware. Users need to exercise care when clicking on links shared in emails, social media and SMSes.

Phishing emails may appear to contain advice about symptoms, medical advice, financial aid, restrictions details or financial guidance. Spelling mistakes are a key characteristic of phishing emails. Emails should be scrutinised before clicking on embedded links and attachments. Readers may unsuspectingly click on links and attachments in order to get more information but may be infecting themselves with malware or linking to malicious sites that capture data. Figure 2 shows an example of a phishing email that falsely claims to link to a list of coronavirus cases in the audience’s area. “You are immediately advised to go through the cases above for safety hazard,” urges the text of the phishing email.

Google says it saw more than 18 million daily malware and phishing emails related to COVID-19 scams just in the week April 16 2020 (Lyons, 2020). Figure 3 shows an example of an email pretending to be affiliated to a user’s organization and prompting for urgent action.



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

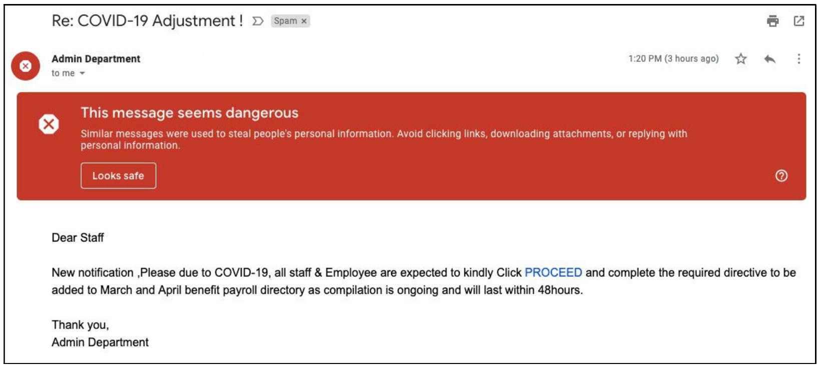
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health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

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

You are immediately advised to go through the cases above for safety hazard

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

Figure 2: Phishing Example Email (Norton 2020)



Re: COVID-19 Adjustment ! Spam ×

Admin Department
to me

1:20 PM (3 hours ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

Dear Staff

New notification ,Please due to COVID-19, all staff & Employee are expected to kindly Click PROCEED and complete the required directive to be added to March and April benefit payroll directory as compilation is ongoing and will last within 48hours.

Thank you,
Admin Department

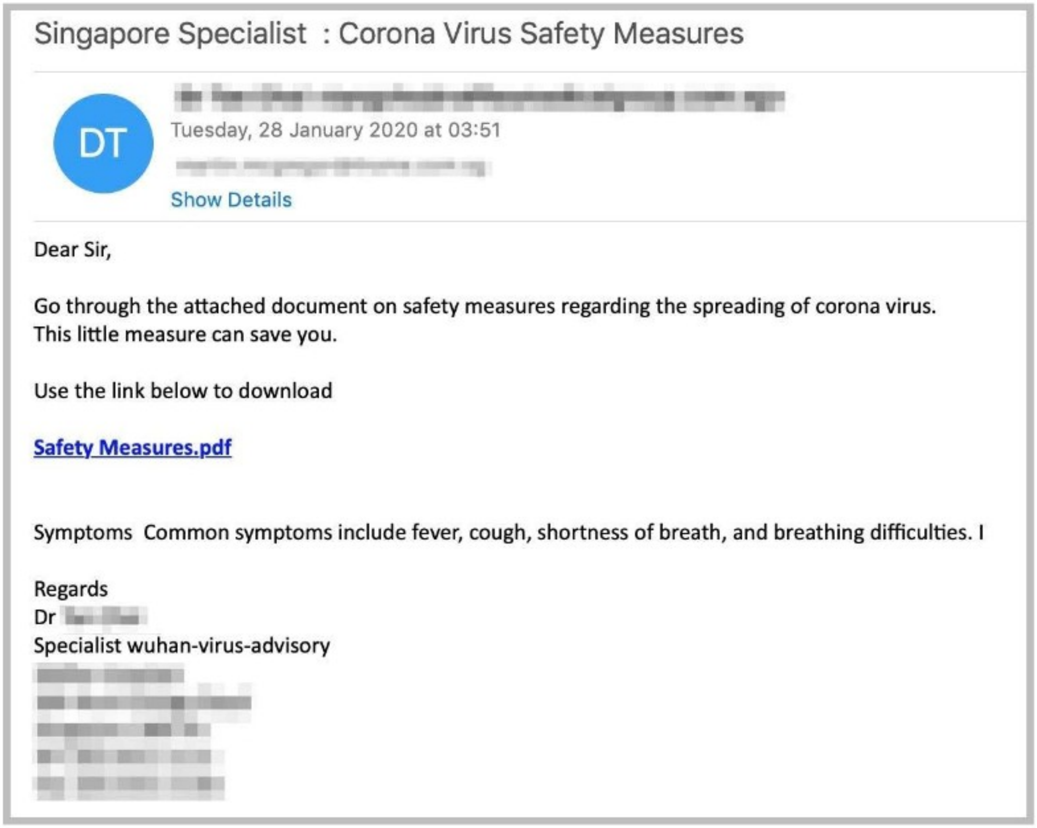
Figure 3: Phishing scam related to Covid-19 (Lyons 2020)

In another elaborate phishing scam, bogus tenders are being advertised by health official for non-existent sanitizer machines (Ritchie 2020). In this scheme the tenders are falsely being awarded, resulting in the applicants investing resources in the execution of the required products/services.

3.2 File Masquerading

Like phishing emails, users may be sent malicious Office Files, system files or application files. These files may be disguised to contain information about the virus and users will eagerly open. These attachments may contain malware and thus by clicking on them, users actually infect themselves. Criminals have started using either non-standard file formats or change extensions of files while storing or transmitting them over a network and this poses a very severe problem for the unauthorized users to send malicious data across the network and it is essential to tackle this e-crime which may harm the entire organization and network (Dhanalakshmi and Chellappan, 2010).

Figure 4 shows an example of fake health advice. The attachment is malicious and users may infect themselves with malware if the link is clicked on.



Singapore Specialist : Corona Virus Safety Measures

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Figure 4: Malicious Download Example (Norton 2020)

3.3 Application Masquerading

While surfing in cyberspace, users may inadvertently infect themselves with malware like scareware, ransomware and rogueware. These types of malware may collect information about users, encrypt their drives or convince them to infect themselves with more malware. In an attempt to gain access to more information and news about Covid-19, users may corrupt their own devices.

Malvertisers have eagerly jumped onto the malvertising bandwagon in order to exploit potential victims during the ongoing Covid-19 pandemic. Cyber-attacks spread through tainted or malicious ads grew as lockdowns came into force around the world in March and hit a peak of more than double the baseline aver-age on 28 March, according to research from AdSecure (Leyden 2020). Leyden further explains that scareware attempts to trick users into buying worthless services or software on the basis that their machines are riddled with non-existent threats and has been a favoured choice of the cybercriminal over March and April 2020.

New research from Microsoft shows that ransomware attackers are actively making that crisis worse; forcing health care and critical infrastructure organizations to pay up when they can least afford downtime (Newman 2020). Ransomware in being released on critical systems with the result that systems are inaccessible, data is stolen and ransom payments are being demanded.

It is important that users carry out safe surfing practices and utilise reputable sites and news agencies to prevent infection. At an organizational level, ransomware defence practices need to be maintained in terms of patching old vulnerabilities, changing default passwords and systems monitoring.

3.4 Web pop-up

While users are engaged in cyberspace web popups may appear prompting users with a media plug-in, error message or questionnaire. Due to these scare tactics or curiosity of users, they may click on these links. Questionnaires can often be bogus and users are duped in filling in information and disclosing details about themselves. Software should only be updated from installed applications and not from pop-ups.

3.5 Malvertisement

Deals for hand sanitisers, face masks and other disinfectants can be sent to users via infected ads and other messages that actually carry out one-click fraud. Users can be instructed to install software on Download Buttons that are actually fake and infect the user.

Consumers are also being exposed to possible counterfeit goods online. By the beginning of May 2020, Amazon has banned more than one million products claiming to protect against or cure an incurable virus and China has confiscated 31 million knockoff face masks (Fast Company 2020). It is important to purchase virus protection equipment from reputable retailers and providers.

3.6 Social Media Injection

Social media is a prime form of communication around the world. Attackers may try to infiltrate users with friend requests, fake video links and malicious games. As users engage in these popular platforms they may fail to see the danger and accept requests or click on links. In the Covid-19 crisis, users may eagerly accept connections from apparent health, news or governmental sources. They also may be enticed with game links. Social media needs to be used with caution.

3.7 Fraudulent Schemes

Covid-19 has created difficult and uncertain times. In turn, fraudsters try to take advantage of the health crisis and try to profit from the urgent need of safety. Various schemes have been devised by fraudsters in order to benefit from the health emergency. These include (KPMG 2020):

- **Fake charities**: During and after disasters like COVID-19, individuals are likely to set up fake websites claiming to be a charity (Waskik 2020). Cyber criminals seeking to take advantage of the pandemic may create fake charities in order to solicit money. Claims can also be made that donations are being used to develop a vaccine against the virus. Phishing sites may be set up to capture users' data as they attempt to make donations. Funds may be channelled into the fraudsters' pockets and not into legitimate charities. It is advised to use reputable web sites and the proper formal channels to make financial contributions. Users should not be misled into handing over their financial information under the guise of aiding this health crisis.
- **Supply scams**: keen to exploit short supplies and urgent demand for certain goods, fraudsters may create online shops selling health and cleaning suppliers like Personal Protective Equipment, face masks, hand sanitizer, bleach and other cleaning materials. Users are misled into believing that they will receive their goods. Items are ordered and payments made. However, the items are never delivered to the consumers.
- **Treatment scams**: Users seeking cures or preventative treatments for the virus may be deceived into purchasing bogus products that claim to remedy their symptoms. Victims may be lured by marketing of vaccines, cures and other treatment products.
- **Provider scams**: In this type of scam, fraudsters claim to be a doctor or hospital administrator that treated a known friend or relative for the virus and demand payment for the treatment rendered.
- **Mobile app scans**: Mobile phone applications are being manipulated and infect users with malware. The application on the surface may appear to be tracking the spread of Covid-19 but in the background it is stealing data like personal information, bank account details and passwords.
- **Investment scams**: The notion of this investment scam, is that it tries to convince users into investing in a company that has services or products that prevent, detect of cure Covid-19. The user is assured significant return on their investment.

Users need to be wary of information that claims to be from experts who have vital information about the virus. Users need to be vigilant and look out for irregularities like spelling mistakes, and strange naming conventions. Proper research should be done before donating to any charity, making a purchase, installation of software and potential investments.

3.8 Wireless

As more users are forced to work remotely in the Covid-19 crisis or practice social distancing and remain at home, users are keen to find Internet access. They may be deceived into using rogue access points in an attempt to get network connectivity with incurring additional costs. These rogue access points may spy on users and steal credentials. Users need to make use of secure wireless connections in order to prevent falling victim to this type of attack.

3.9 Video-conferencing

Businesses and educators rely on digital technology to maintain communications during lockdown. There has been a widespread increase in the ability to collaborate and connect digitally as users no longer have access to face-face meetings. Zoom has reported a 20-times growth in daily participants with voice calls in some countries having tripled, and the use of communications apps have doubled (O' Halloran 2020). Virtual conferences, video calls, video meetings and webinars are all tools that have become indispensable. Video-conferencing, however can be vulnerable to exploitation. As more employees require video conferencing capabilities, cyber criminals may send out false video conferencing invites. Users cannot afford to ignore important work meetings and thus can be falsely lured into clicking on the links which may not be legitimate meeting notifications. Some organisations have organisational specific video-conferencing software and thus users are advised to follow organisational policy and recommendations in this regard. In addition, meeting notices should not be shared with third parties that do not have permission to attend a meeting. Passwords or tokens can also be used in order to control access to online meetings. Passwords can be distributed to all legitimate invitees and have to be entered before being allowed access to meeting. A token is an individual code that allows a user to join a meeting. It is the most secure method as once a user enters their token it cannot be re-used.

Internet trollers may try to hack into online meetings in order to hijack, interfere or eavesdrop on meetings. "The FBI said it received multiple reports of so-called "Zoom-bombing," including some disturbing incidents in online classrooms. In Massachusetts, for example, uninvited guests yelled profanity and displayed swastika tattoos during school video chats "(Jokich in Zielinski 2020). The attendees should be carefully checked and monitored in order to ensure that only valid participants join into online meetings.

During a video conference, users should check that their cameras are disabled when not required. Information may be disclosed unwittingly and thus exercise care when making use of these digital capabilities.

3.10 False information

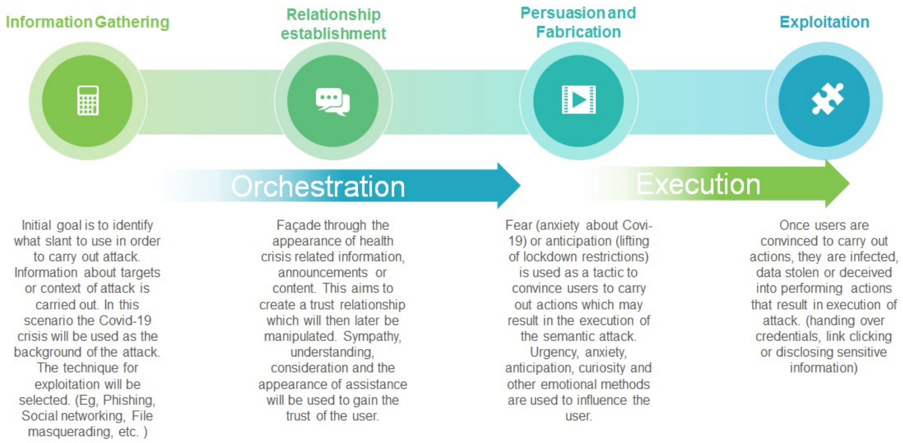
In many countries, it is a legal offence to spread false information about Covid-19. Those infringing this law are liable for prosecution. Exaggeration of statistics, misinformation about diagnosis, cures, regulations, guidelines, emerging news are all ways in which Covid-19 information can be incorrectly communicated. False information can lead to panic, anxiety, heightened fear and hysteria. Thus, information published and spread should be verified before users can deem content as true. It is important to trust authoritative sources and not solely rely on social media links, forwarded messages and information published on independent web sites. As World Health Organization Director-General Tedros Adhanom Ghebreyesus rightly said in February, "We're not just fighting an epidemic; we're fighting an infodemic" (Hazelton 2020). Some important tips to help identify false information:

- As more data studies are carried out, increased information will be revealed. Any reputable scientific source will endeavour to present the information as accurately as possible at that point in time. Some scepticism may have to be applied to statements that merely state "scientific evidence prove that…" It is important that the information be cited from a sound source or actual study.
- Information may appear to be based on scientific findings but this may not necessarily be true. Data may be reported, analysed, interpreted in many ways- all of which may not be scientific. Information from an original source (the data study) may be re-interpreted, reported on and modified. Information should be verified across multiple media outlets.
- Many scientists are making comments and are being interviewed. However, it does necessarily mean they are qualified in the field of virology or epidemiology. It is important to be aware of potential conflicts of interest or how the comments could potentially benefit certain parties. Opinion pieces may potentially try to sway users' views. Users need to be discerning when coming across different forms of information regarding the virus. Users need to rely on trusted sources and proper evidence-based information.

3.11 Approach to Attacks

The previous section looked at providing key examples of how users can be exploited based on the Covid-19 crisis. It would also be beneficial to find the mutual elements of attacks in order to identify when a potential attack is being launched.

In 2013 Tetri and Vuorinen introduced a dynamic classification frame- work that addresses high-level attack behaviours involved in the creation of a semantic attack: persuasion, fabrication and data gathering. With reference to the execution of a social engineering attack, Allen (2006) identifies the steps as Information gathering, Developing Relationship, Exploitation and Execution. The data gathering from Tetri and Vuorinen is comparable to the data that is gained from the execution step of Allen. Heartfield and Loukas (2015) in their taxonomy of attacks propose three stages as orchestration, exploitation and execution. Figure 5 shows the adaptation of these various frameworks in order to summarise the approach of how attackers carry out social engineering attacks with a focus on semantic attacks in the context of Covid-19. It endeavours to show the mutual elements of an attack and aims to help with attack identification and prevention.



Initial goal is to identify what slant to use in order to carry out attack. Information about targets or context of attack is carried out. In this scenario the Covid-19 crisis will be used as the background of the attack. The technique for exploitation will be selected. (Eg, Phishing, Social networking, File masquerading, etc.)

Façade through the appearance of health crisis related information, announcements or content. This aims to create a trust relationship which will then later be manipulated. Sympathy, understanding, consideration and the appearance of assistance will be used to gain the trust of the user.

Fear (anxiety about Covi-19) or anticipation (lifting of lockdown restrictions) is used as a tactic to convince users to carry out actions which may result in the execution of the semantic attack. Urgency, anxiety, anticipation, curiosity and other emotional methods are used to influence the user.

Once users are convinced to carry out actions, they are infected, data stolen or deceived into performing actions that result in execution of attack. (handing over credentials, link clicking or disclosing sensitive information)

Figure 5: Covid-19 Approach to Semantic Attacks

Initially during the orchestration of an attack, an attacker will gather information pertaining to target selection and the technique for execution. This will entail the development of the storyline or creation of the context from which the attack will be launched. In the Covid-19 case users' interests for information, news and updates is preyed upon. There is strong need for information relating to the virus, new statistics, health information, governmental announcements and lockdown restriction issues. The stay home campaign also resulted in more users engaging on the Internet for entertainment and leisure. Due to the dependencies for network access, this avenue of providing connectivity for users can also be used for manipulation. Exploits can be orchestrated in a number of ways including Phishing, File Masquerading, Social Networking, etc. These types of techniques are used to package the exploit and deceive the user.

The attacker will try to establish a relationship with the victim by fabricating a scenario and persuading the user into carrying out actions. Users can be lured by material that relates to the Covid-19 virus. This then leads to the execution of exploitation whereby the user is tricked into the exploit due to the urgency or enticement created in the storyline. Users fall victim to the exploit and then ex-pose themselves to infection, theft or disclosure.

4. General Concerns

Overall, the Covid-19 pandemic has created various trying conditions where users are increasingly reliant on network, remote and Internet access. This has introduced additional cyber security concerns and will be discussed next. This sections aims to show users how security in general can be overlooked.

4.1 Weakened End-point Security

In an effort to curb the spread of the Covid-19 virus, many employees began to work remotely from their homes. Users were thus operating from their home offices. However, many organisations build up a cyber-security perimeter within their organisations. Organisational policy will prescribe updates, security tools, technologies and measures to protect the network. While working remotely users may not have the same level of protection. In an organisation, users' devices may be located in a firewalled environment with regular scanning and detection of anomalous behaviour. However, users in the home setting may not be afforded these organisational benefits. Users' devices may lack firewalls, anti-virus software, anti-spyware and intrusion detection capabilities. Not all organisations have Virtual Private Networks (VPNs) set up and thus data may be transmitted in the clear without security concerns. Updates may not be carried out and users may be using outdated software with security vulnerabilities and backdoors.

4.2 Confidentiality

Users may operate unencrypted devices while working with sensitive data. When working on home devices users may overlook security issues for ease of use and convenience. Sensitive data may be stored in the open on backup hard drives or saved to cloud services. The confidentiality of the data may be compromised if the data is leaked or intercepted. Emails may be sent regarding sensitive data in an unencrypted format. Strong password security may not be enforced on personal devices that are being used to support business operations. In an effort to continue business operations, users may overlook security issues and make use of insecure methods of operating.

4.3 Remote Exploits

Linked to the corona virus, one of the cyber trends identified by the cyber security company Cynet is the stealing of remote user credentials (IOL 2020). Mcaffee has found that there has been significant growth in the number of attacks targeting Microsoft's Remote Desktop Protocol (RDP) during the Covid-19 pandemic (Graw 2020). Attackers could use this opportunity to gain access to users' sensitive data and systems, as well as to unleash malware. Remote access exploitation could expose an entire business network. It is important to limit remote access connections over an open network, use complex passwords and make use of multi-factor authentication.

5. Conclusion

The Covid-19 pandemic created extenuating conditions, which radically changed the workplace, as well as leisurely engagements. Employees were required to work from home and everyone was encouraged to practice social distancing. This in turn resulted in increased use of the Internet and cyberspace to work, socialise, connect and communicate.

This paper addresses common semantic attack vectors relevant to the Covid-19 virus. It aims to show how attackers may exploit this health crisis in order to take advantage of users in order to elicit information, spy on users, take control of systems, steal funds and other malicious actions. It is hoped that through the paper awareness is created on critical attack paths that attackers may use to leverage users data and resources.

6. References

Allen, M. (2006). Social Engineering: A Means to Violate a Computer System. Bethes-da, MD: SANS Institute.

Bisson, D. (2019) 5 Social engineering attacks to watch out for. The state of security. [Online]. Available at: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/ (Accessed 7 May 2020)

Dhanalakshmi, R. and Chellappan, C. (2010) Detection and Recognition of File Masquerading for E-mail and Data Security, Communications in Computer and Information Science book series (CCIS), Vol. 89, . [Online]. Available at: https://link.springer.com/chapter/10.1007/978-3-642-14478-3_26

Fast Company, (2020). The growing problem of fake goods in the Covid-19 era, . [Online]. Available at: https://www.fastcompany.co.za/business/fake-goods-are-a-problem-in-the-covid-19-era-47562218, (Accessed 7 May 2020)

Graw, M. (2020) McAfee finds hackers targeting Remote Desktop Protocol during Covid-19, . [Online]. Available at: https://www.techradar.com/uk/news/mcafee-finds-hackers-targeting-remote-desktop-protocol-during-covid-19, (Accessed 11 May 2020).

Hazelton, A. (2020) How to read the news like a scientist and avoid the COVID-19 'infodemic', [Online]. Available at: https://www.weforum.org/agenda/2020/03/how-to-avoid-covid-19-fake-news-coronavirus/ (Accessed 20 April 2020)

Heartfield, R. and Loukas, G. (2015) A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks, ACM Computing Surveys (CSUR), Vol 48, Issue 3, . [Online]. Available at: https://dl.acm.org/doi/pdf/10.1145/2835375

IOL. (2020) Spike in cyberattacks as cyber criminals exploit Covid-19 lockdown, [Online]. Available at: https://www.iol.co.za/technology/software-and-internet/spike-in-cyberattacks-as-cyber-criminals-exploit-covid-19-lockdown-report-46424508 (Accessed 11 May 2020).

Kapersky (2020), Social Engineering Definition, [Online]. Available at: https://www.kaspersky.co.za/resource-center/definitions/what-is-social-engineering (Accessed 17 April 2020)

KPMG (2020) Beware of Covid-19 frauds and scams, [Online]. Available at: https://home.kpmg/vn/en/home/insights/2020/04/covid-19-frauds-and-scams.html (Accessed 7 May 2020)

Leyden, J. (2020) Malicious advertising slingers up the ante during Covid-19 pandemic, [Online]. Available at: https://portswigger.net/daily-swig/malicious-advertising-slingers-up-the-ante-during-covid-19-pandemic (Accessed 7 May 2020).

Luo, X. Brody R. Seazzu, A. & Burd, S. (2011) "Social Engineering: The Neglected Human Factor for Information Security Management," Information Resources Management Journal (IRMJ), IGI Global, vol. 24(3), pages 1-8, July, 2011.

Lyons, K. (2020) Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week, [Online]. Available at: http https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams (Accessed 8 May 2020)

Newman L.H. (2020) The Covid-19 Pandemic Reveals Ransomware's Long Game, [Online]. Available at: https://www.wired.com/story/covid-19-pandemic-ransomware-long-game/ (Accessed 7 May 2020)

Norton, (2020) Coronavirus phishing emails: How to protect against COVID-19 scams, [Online]. Available at:https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html, (Accessed 7 May 2020)

O' Halloran, D. (2020) 5 ways to protect critical digital connectivity during COVID-19, World Economic Forum, [Online]. Available at: https://www.weforum.org/agenda/2020/04/covid-19-5-ways-to-protect-critical-digital-connectivity/ (Accessed 20 April 2020)

Readfearn, G. (2020) How did coronavirus start and where did it come from? Was it really Wuhan's animal market?, [Online]. Available at: https://www.theguardian.com/world/2020/apr/15/how-did-the-coronavirus-start-where-did-it-come-from-how-did-it-spread-humans-was-it-really-bats-pangolins-wuhan-animal-market, (Accessed 15 April 2020)

Ritchie, G. (2020) Fraudsters claiming to be health department officials are peddling tenders for a non-existent sanitiser machine, [Online]. Available at: https://www.dailymaverick.co.za/article/2020-05-05-gone-phishing-business-owner-almost-scammed-by-fake-covid-19-tender/ (Accessed 7 May 2020)

Tetri, P. and Vuorinen,, J. (2013) Dissecting social engineering. Behaviour and Information Technology Vol 32, No 10, pg. 1014–1023.

World Health Organisation. (2020) Beware of criminals pretending to be WHO, [Online]. Available at: https://www.who.int/about/communications/cyber-security (Accessed 7 May 2020)

Wasik, J.F. (2020) This Is How You Avoid COVID-19 Charity Scams, [Online]. Available at: https://www.forbes.com/sites/johnwasik/2020/04/08/this-is-how-you-avoid-covid-19-charity-scams/#52aa91407a68 (Accessed 7 May 2020)

Workman, M. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat. Information System Security, Vol 16, No6, pg. 315–331. doi:10.1080/10658980701788165.

Zielinski, D. (2020) Video Calls Gone Wrong? How to Avoid Bombing Your Virtual Conference, [Online]. Available at: https://blog.clickmeeting.com/simple-ways-to-secure-your-virtual-conference (Accessed 20 April 2020).