الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies

Cybersecurity Quarterly Bulletin

Q1 2020

Classification: Open

TLP: White

Contents

Highlights from the Quarter

Q1 2020 (January-March)

Q1 2020 has been marked by COVID19, and the global emergency has brought consequences for cybersecurity. Teleworking (remote working) this global emergency has brought overnight, with little preparation for workers and organizations. Cyber-threats have been exploiting the widened attack surface, and the situation is bound to continue as threat-sources adapt social engineering attacks to capitalize on the public fear of the pandemic and the resulting economic crises.

In the meantime, the Saudi National Cybersecurity Authority organized the Global Cybersecurity Forum, the biggest and most important cybersecurity event ever held in the region.

Bits and Bytes

Key quarterly statistics, top threats and targeted sectors globally

Expected number of teleworkers during the COVID crisis

300,000,000+

Telework jumped from 27% to 60% as of March 2020. In Italy alone – where lockdown measures have been strict –A 775% month-on-month activity increase was observed on collaboration platform. [1]

Insecure devices linked to corporate networks

1,000+ everyday

Companies across Europe and North America have estimated a sharp increase of insecure personal devices newly connected to enterprise networks without the knowledge of organizations' IT departments. [2]

Malicious COVID19 website

9 out of 10

Between 9-23 March, 315,000+ COVID19-themed websites have been created. Of these, nine out of ten are malicious or connected to frauds or scams. [3]

Cost for ready-to-use COVID19 malicious map

750 SAR on average

Cybercriminals are selling COVID19 phishing tools such as interactive maps that show legitimate data about the COVID19 spread, but are equipped with malicious payloads. [4]

Top 5 targeted sectors globally in Q1 2020[5]

1. Public - 21,58%
2. Healthcare - 13,37%
3. Education - 12,16%
4. Finance - 11,55%
5. Manufacturing - 7,29%

Top 5 global threats in Q1 2020[5]

1. Malware - 42,09%
2. Account Hijacking - 19,66%
3. Targeted Attack - 11,97%
4. Vulnerability - 6,20%
5. Malicious Spam - 4,70%

Top 5 threats in KSA in Q1 2020[6]

1. Malware –
2. Unauthorized access / Modification -
3. Penetration/attempt to penetrate –
4. Incorrect use-
5. Data leakage -

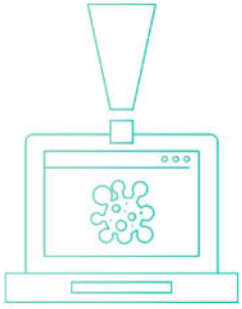
[1] BGC, Managing the Cyber Risks of Remote Work, March 2020.
[2] Deloitte, Deloitte Global Cyber COVID19 weekly executive cyber briefing, March 2020
[3] Forbes, Google Data Reveals 350% Surge In Phishing Websites During Coronavirus Pandemic, March 2020
[4] Digital Shadows, How cybercriminals are taking advantage of COVID-19, March 2020
[5] Numbers show the distribution (%) over the total number of attacks registered worldwide for Q1
[6] NCA analysis. Numbers show the top cybersecurity threats registered in the Kingdom of Saudi Arabia for Q1.

Global Cyber Outlook

Cybersecurity headlines from around the world

COVID19 themed campaigns and implications for the World Health Organisation

Researchers are identifying many COVID19-themed cyber campaigns around the world, which capitalize on peoples' fear of the pandemic. The World Health Organization (WHO) is at the center of many of these campaigns, as a victim of targeted cyber-attacks (with attackers attempting to access WHO staff accounts to exfiltrate data about COVID19 vaccines and medicines)[7] but also as an indirect victim of impersonation attacks.



Since the beginning of the crisis, there has been a surge of malicious campaigns from attackers posing as the WHO with the purpose of obtaining money (e.g. through fake donations) or credentials (e.g. through fake subscription services). The situation is so serious that the WHO has issued an official statement warning about these social engineering campaigns. This technique has also been replicated in similar attacks, involving institutions like the U.S. Center for Disease Control and Prevention (CDC), or the United Nations International Children Emergency Fund (UNICEF).[8]

Cyber Threat targeted at Healthcare and the response from the Cyber Community

Cyber threats and attacks have re-focused their efforts around COVID19-themed campaigns and, in particular, against the healthcare sector.[9] The focus on the healthcare sector by many cyber-threats is a source of concern around the world. Globally, this sector is already experiencing great operational stress in its attempt to contain the health emergency. This means operators are struggling to infuse the necessary resources to protect hospitals, medical professionals, and patients. Despite the claims of some cybercrime groups not to target the healthcare sector during the COVID-19 emergency, attacks have spiked, posing a risk on the effectiveness of prevention, treatment and response to the pandemic.[10]

[7] Reuters, Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike, March 2020.
[8] WHO, Beware of criminals pretending to be WHO.
[9] Deloitte, The rise of cyber threats in March and April amid COVID-19, April 2020; Deloitte, Global Cyber COVID-19 weekly executive briefing. Issue 3, April 2020
[10] Forbes, Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis, March 2020; Interpol, Cybercriminals targeting critical healthcare institutions with ransomware, April 2020.

National Cyber Outlook

Cybersecurity headlines regarding the Kingdom of Saudi Arabia

The G20 Cybersecurity Dialogue

As part of the Kingdom's efforts to support cybersecurity priority in the Kingdom's presidency for the G20 summit, the Kingdom held The Cybersecurity Dialogue on February 3-2020 in alignment with the first meeting of the Digital Economy Task Force as an official side event in the G20's agenda.[12]

The dialogue aims to enhance the discussion on cybersecurity in various sectors, broaden the discussion on the priority of cybersecurity in the path of the digital economy and discuss innovative ideas for capacity building and interaction with private sectors and with emerging economies. The event was attended by a selection of stakeholders including representatives of the G20 Digital Economy Task Force , and a number of B20 representatives, including representatives from leading private sector companies and advanced technologies, global thought leaders, and international organizations.

Saudi Arabia hosted the Global Cybersecurity Forum

On 4-5 February 2020, Saudi Arabia's National Cybersecurity Authority hosted the Global Cybersecurity Forum (GCF) in Riyadh, under the patronage of the Custodian of the Two Holy Mosques King Salman Bin Abdulaziz Al Saud, the largest cybersecurity event held in the Middle East to date. It brought together more than 3.500 participants from over 58 countries, including government officials, academics and business leaders to discuss global cybersecurity. Over two days, attendees had the chance to attend panels and discussions on the cybersecurity industry, emerging threats and risks, resilience, security behavior, and international collaboration.

Numerous side events and meetings held between local authorities and national, regional, and international stakeholders completed the event. During these, meetings the NCA signed five major *Memoranda of Understanding* to bolster collaboration with national and international partners and to further reinforce the Kingdom's cybersecurity stance.[13]

Riyadh Declaration for Cybersecurity

During the GCF, the NCA launched the "Riyadh Declaration for Cybersecurity". The document recognizes the opportunities of connected global systems and evolving technologies, and emphasizes the central role played by a thriving cybersecurity industry and workforce, responsible communities, cyber resilience, and inclusive capacity building in shaping the state of cybersecurity globally

The declaration can be accessed at globalcybersecurityforum.com/declaration

[12] G20 official website
[13] Global Cybersecurity Forum , Five prominent MoUs signed at the Global Cybersecurity Forum, February 2020.

Top Security Stories

A look at prominent cybersecurity events from the last quarter

WHO-themed campaigns [14]

Location: Worldwide

Sector: International Organization, Healthcare

Date of disclosure: February 2020

Type of attack: Multiple attacks (phishing, website spoofing, keylogger, etc.) using social engineering techniques

Description: On 11 February, the WHO warned of cyber campaigns online and on instant messaging apps, in which criminals contacted victims pretending to be WHO staff, with the purpose of obtaining credentials or sensitive information from the victims.

These attacks increased, mostly revolving around phishing emails with links leading to malicious websites or containing malware in the form of fake attachments. These emails appear not to be targeted to specific individuals and are often crafted with low attention to detail (e.g. containing spelling and grammar mistakes).

In many instances, the attackers combined phishing email with web spoofing. Web spoofing is a type of attack in which hackers replicate a legitimate website, mimicking all of its contents and its design, in order to persuade victims that the website is legitimate.

Among the payloads (i.e. the item or portion of code that performs the intended malicious action) that have been identified in these WHO-themed campaigns, security researchers noted that one of the most common is the infamous AgentTesla malware. This malware is misspelled, which works by registering the keyboard strokes of the users and capturing what the victims write, including password and sensitive information.

Impact: Compared to Q1 of 2019, in the first quarter of 2020 the total number of cyber-attacks (both those against the WHO's personnel, and those in which attackers pose as WHO staff) has been five times higher, creating an additional operational strain on top of other COVID19 activities.

Lessons learned: In times of crisis it is crucial to have clear governance that is capable of managing both the primary crisis (in this case, a health one) and its cybersecurity implications. During such crises, organizations should:

- Maintain a heightened level of attention and monitor attentively cyber threat landscape in order to identify malicious campaigns that legitimate organizations.
- Immediately communicate the detected social engineering campaigns and raise awareness about it.
- Raise cybersecurity practices in how to respond to such risk.

[14] WHO, Beware of criminals pretending to be WHO; CISA, Defending Against COVID-19 Cyber Scams, March 2020; Bleeping Computer, World Health Organization Warns of Coronavirus Phishing Attacks, February 2020; Sophos, Coronavirus "safety measures" email is a phishing scam, February 2020; Fortinet, Latest Global COVID-19/Coronavirus Spearphishing Campaign Drops Infostealer, April 2020; Carbon Black, Technical Analysis: Hackers Leveraging COVID-19 Pandemic to Launch Phishing Attacks, Fake Apps/Maps, Trojans, Backdoors, Cryptominers, Botnets & Ransomware, March 2020; Proof Point, Attackers Expand Coronavirus-Themed Attacks and Prey on Conspiracy Theories, February 2020.

Cyber Secure

The COVID19 crisis demonstrated how the working environment can change suddenly.

The following tips provide guidance to business owners on how to prepare for such scenarios15

Tips for the Management

Prepare for the crisis

- Ensure cybersecurity standards and controls are documented and implemented [16]
- Identify the organisation's critical assets and ensure cybersecurity controls are applied accordingly.
- Define a business continuity plan for mission critical assets.
- Identify the organisation's services and personnel that need to work on-site, can work remotely, or can suspend working activities in times of crisis.
- Identify a "crisis management team" responsible for urgent circumstances. Ensure it has the needed capabilities from the business side and supporting areas (e.g. IT, legal).
- Ensure organisation's network is scalable to support the emergency needs (e.g. high volume of data due to teleworking, VOIP, remote desktop, etc.). Assess it by means of testing and simulations.
- Consider specific testing scenarios for business continuity that will simulate the organisation's operations during a crisis.
- Periodically review crisis plans.

Act swiftly during crises

- Activate the "Crisis Management team ".
- Verify that the organization's technical infrastructure and applications are updated and patched.
- Personnel devices that meet cybersecurity requirements must be provided to ensure secure remote working.
- Activate dedicated communication channels (e.g. "hotline") to support staff in the transition to telework (e.g. setup devices, check the cybersecurity requirements, etc.).
- Adopt solutions to support telework (e.g. video conferencing). Ensure such technologies comply with cybersecurity requirements.

Tips for the Staff

- Become familiar with the organization's Crisis plan.
- Ensure using a secure network, all of the connected devices are updated, and that have sufficiently strong authentication mechanisms.

Your awareness is your weapon that will help protect your information, devices and privacy. Saudi CERT launched guidelines for employees, providing:

- Best practices to fortify your personal account against security risks
- Establishing a "Home Office" Environment
- Best practices to fortify internal working systems
- Teleworking security when moving and traveling
- Be aware and know the danger signs

[15] The present guidelines and tips have been prepared by the Saudi Arabia National Cybersecurity Agency, taking also into account suggestions from renowned organizations such as the US National Institute of Standards and Technologies (NIST SP 800-53 Security Controls and Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security 800-46), the SANS Institute (Pandemic Response Planning Policy, 2020), the French Commission nationale de l'informatique et des libertés (Les conseils de la CNIL pour mettre en place du télétravail), The US Department of Homeland Security (Trusted Internet Connections 3.0 Interim Telework Guidance), and DELOITTE (COVID-19: Cyber and the remote workforce).

[16] For an efficient way to define organization's baseline cybersecurity, please refer to the Saudi Essential Cybersecurity Control from the Saudi Arabia National Cybersecurity Agency.

Looking Ahead: New Trends

COVID19 is likely to cause lasting impacts, and technology will be an engine for recovery. The section looks at possible future scenarios and the expected impact on cybersecurity

Scenario 1: Teleworking our way out of the crisis

Containment measures will affect this scenario in two possible ways:

1. Teleworking declines to the pre-crisis level. This will occur if the crisis and its consequences to the economy are "V" shaped, with a steep downfall and a quick bounce back (6-12 months), or

2. Teleworking lives on. Workers will acclimatize and organizations realize its value beyond the emergency. The longer lockdown lasts, the higher the chances that teleworking continues.

Option 2 is more likely (though telework will not become the primary way of working) and will widen the attack surface.[17] Since home networks are less protected than corporate ones, cybercriminals will focus their attacks against the former.

Organizations will ramp up security solutions and provide training programs to increase employee security awareness to work remotely secured.

Scenario 2: New business landscape, new risks, new opportunities

COVID19 is impacting the business landscape in two ways.

1. Changes to existing businesses. Some companies that manufacture medical products (e.g. ventilators, surgical masks, sanitizer) or provide services (e.g. hospital logistics) essential to fight COVID19 are being included as part of the important national infrastructure on a global level.[18] Most are not prepared for the higher cybersecurity threshold required by this status. Thus, they need to invest in cybersecurity to ensure compliance, further strengthening the global cybersecurity market. The opportunity exists for the business players in the sector to position themselves with cybersecurity as a competitive advantage.

2. Creation of new health businesses and services. It is expected that the current high expenditure on health products (since the beginning of the emergency, online purchase of cold, cough and flu products alone registered over +190%) will continue on a mid to long term basis, affecting medical services as well. Telemedicine and remote medical counseling will boom, placing a lot of sensitive and lucrative health data online (the value of such data is 5000% higher than the value of personal information), at risk of theft by cyber-threats.[19]

Scenario 3: The growth of the cybersecurity market

The combined effect of increased cyber threats and increased reliance on technology will encourage the evolution of certain segments of the cybersecurity products and services market.

According to estimates, the cybersecurity technology market alone is expected to grow from approx. 688 billion SAR in 2019 to over 863 billion SAR by 2021. Endpoint protection, detection, and response will see the most significant growth, due to the updates that a large number of organizations will have to perform to accommodate the needs of remote working. For the same reason, it is likely that networking and connectivity solutions will see similar growth.[21]

[17] Deloitte, COVID-19: People, technology, and the path to organizational resilience, 2020
[18] Deloitte, The essence of resilient leadership. Business recovery from COVID-19, 2020
[19] The Nielsen Company, Key consumer behavior thresholds identified as the coronavirus outbreak evolves, March 2020; Deloitte, Global Cyber COVID-19 weekly executive briefing. Issue 3, April 2020; The Financial Times, Lockdown drives boom in healthcare apps, May 2020.
[20] Markets and Research, Covid-19 Impact On Cybersecurity Market by Technology (Network Security, Application Security, Endpoint Security, Cloud Security, Database Security, Web Security, ICS Security), Vertical, Region - Global Forecast to 2021.

Spotlight on Cyber Innovation

This provide recommendations to increase the protection of smart cities.

The advancement of smart cities, and their integrated infrastructure, makes them powerful assets to fight outbreaks.

Key recommendations to increase the cybersecurity resilience of smart cities. To strengthen smart cities to resist, and be resilient to, cyber threats, recommendations include:

Establish a cybersecurity framework for the city

Identify stakeholders and follow cybersecurity policies and controls

Implement city-wide detection and response (e.g. Municipality CERT)[27]

Promote cyber awareness and culture among the citizens

Exchange cybersecurity information with other smart cities

Identify core infrastructure elements and protect them

Emphasize the protection of data

This quarterly bulletin has been compiled by the National Cybersecurity Authority (NCA) of the Kingdom of Saudi Arabia (KSA). Its goals are to provide readers with an overview of the most important cybersecurity events and data from the quarter and to highlight the most interesting facts related to the focus of this issue. Aiming to :

- Elevate Cybersecurity knowledge and capabilities
- Provide outlook on latest cybersecurity trends, threats & risks

This report contains the information from several parties and individuals, noting that all information included in the report is indicative only. Also, the NCA does not bear any responsibility - under any circumstances - towards any party as a result of any decision or action taken or will be taken by that party based on the content of this report. The NCA asserts that it is not completely or partially responsible for any direct or indirect prejudice may occur.

About the NCA

The National Cybersecurity Authority (NCA) was established in 2017. The NCA is the government entity in charge of cybersecurity in Saudi Arabia and it serves as the national authority on all related affairs. It has both regulatory and operational functions related to cybersecurity and works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities

© 2020. National Cybersecurity Authority of the Kingdom of Saudi Arabia. Center For Cybersecurity Strategic Studies

https://nca.gov.sa/ @NCA_KSA