SAM
Rights & Liberties

DIGITAL SECURITY IN YEMEN
REALITY AND THREATS

DECEMBER 2022

www.samrl.org

DIGITAL SECURITY IN YEMEN.
REALITY AND THREATS

SAM
Rights & Liberties

Digital Rights Project

A non-profit human rights window affiliated with SAM Organization, with the support of Internews, aims to introduce digital rights and monitor digital violations against users of the digital space, as it works to advocate for the digital rights of Yemenis, with the aim of reaching a safe, fair and free digital space. The window allows reporting digital violations, documenting them and creating a database about them. She publishes studies and research on digital activism, digital rights and digital security, in addition to planning and managing local and international advocacy campaigns.

violations@samrl.org

Introduction

Talking about digital security is not a luxury, as much as it is an urgent necessity imposed by the steady development of technology and the accompanying threats and risks, which the most powerful technological empires are sometimes unable to address, let alone a country with a fragile and very weak cyber capacity, such as Yemen, which occupies the bottom of the classification in the Global Cybersecurity Index.

Internet users in Yemen face real risks and threats ranging from censorship and external espionage, hacking attacks, malware attacks, and social media phishing, which takes deceptive patterns, such as fake Facebook pages, messages attached to malicious links, and other methods targeting victims in Yemen.

In this report, we will discuss the reality of digital security in Yemen, based on indicators and statistics on the magnitude of threats and risks faced by Internet users. We will also address mechanisms and procedures to enhance information security, at the institutional and individual levels.

Conceptual framework

-Digital Security

A collective term that describes the resources used to protect your identity, data, and other online assets, including web services, antivirus software, smartphone SIM cards, biometrics, and secure personal devices. Simple Learn.

- Cybersecurity

It is the practice of protecting systems, networks, and programs from digital attacks, which usually aim to access, alter or damage sensitive information, or extort money from users via ransomware. Cisco

Organizational context

Yemen lacks a law regulating the digital space, not to mention the absence of a national cybersecurity strategy, but there are legal provisions on the protection of information and the protection of privacy, which were addressed in draft law No. (13) of 2012, which (has not been implemented).

It is worth noting that the National Cybersecurity Strategic Plan, which resulted from the First National Cybersecurity Conference, held in Sana›a during the period (7-9) June 2021, is the only framework in this regard, and it included guidelines on approving individual cyber protection laws and developing a national plan to respond to cyber incidents. In addition to developing a program to protect the country›s vital information assets and infrastructure, and exemplary governance to manage the implementation of the National Cybersecurity Strategy, as well as, setting cybersecurity laws and regulations, e-transactions and e-commerce.

Digital Security Index

Yemen is one of the worst countries in the Global Cybersecurity Index, due to its lack of technological infrastructure, and according to the Global Cybersecurity Index (GCI) issued by the International Telecommunication Union periodically every two years, to classify the cybersecurity capabilities of countries, Yemen ranked 22nd in the Arab world, and 182nd globally (out of 182 countries) in the Global Cybersecurity Index for the year 2020, after it was ranked 21st in the Arab world, and 172nd in 2018.

The index measures countries› commitment to cybersecurity, identifying their gaps, and assesses the level of development or participation of each country based on five pillars: legal measures, technical measures, regulatory measures, capacity development, and cooperation.

According to the 2020 assessment issued by the e-Governance Academy (NCSI (a non-profit organization that assists public sector organizations around the world in digital transformation), Yemen achieved only 6 indicators out of 77 indicators on which the classification was based, in assessing the country›s cyber capabilities, and they were distributed as follows: general cybersecurity indicators (1 out of 27 indicators), basic cybersecurity indicators (2 out of 24 indicators), and incident and crisis management indicators (3 out of 26 indicators).

Yemen ranked 22nd

in the Arab world and 182nd globally (out of 182 countries) in the Global Cybersecurity Index for the year 2020.

General cyber security indicators

0% Developing a cyber security policy
0% Cyber Threat Analysis and Information
0% Education and professional development
17% Contribution to global cyber security

Basic cyber security indicators

0% Protection of digital services
0% Protection of basic services
11% Electronic identification and trust services
25% Personal data protection

Incident and crisis management indicators

50% Response to cyber incidents
0% Cyber crisis management
0% Fighting cybercrime
0% Cyber Military Operations

Factors of vulnerability and fragility

Recorded Future, an independent intelligence provider to organizations around the world, has found multiple cases of suspicious activity within Yemen›s internet infrastructure, where the IP address of one of YemenNet›s (ns1.yemen.net) main name servers appears to contain a «tenda-backdoor» module, which refers to a firmware backdoor that uses the CVE-2017-16923 vulnerability to perform remote command execution in router models manufactured by Chinese network manufacturer Tenda. Governmental and non-government take advantage of this back door to infiltrate the ISP.

In addition, the Houthi-controlled web hosting servers 82,114,162.66 and 82,114,162.10 – the Houthi-controlled web hosting servers that as of June 2018 hosted more than 500 Yemeni government and educational websites and companies, are riddled with legacy vulnerabilities such as CVE-2003-1582, CVE-2009-2521, CVE-2008-1446, and other older issues that, if left unrepaired, could allow attackers easy access to said systems. Recorded Future - November 2018.

In this regard, the Public Telecommunications Corporation (PTC) revealed, in August 2017, that the national Internet network has been subjected to international hacking that has affected many countries of the world, including Yemen, and caused the cancellation of the settings of ADSL modems for some subscribers, which required reconfiguring and updating modems, in order to re-receive the service. Al-Masirah TV also reported (dated September 2021) that Yemeni telecommunications were subjected to a spying operation, from a number of British ships via the submarine cable off Al-Ghaydah, adding that they stole the data of the Yemeni telecommunications company, in a spying operation that included the whole of Yemen.

According to a January 2018 report by Duke University›s AGS program, experts agree that both YemenNet and Aden Net are full of security vulnerabilities.

Engineer and expert in information technology Ali Al-Saghir Farhan stressed that Yemen›s record in information security is low for several reasons, including: the lack of a cadre specialized in information (cyber) security, the lack of interest of state leaders in the information and communications security sector in a sufficient manner, and the lack of a government agency specialized in providing defense and security services to cyberspace. In addition to the lack of integrated and modern legal frameworks and legislation that establish an effective national base for national cybersecurity, as well as the weak coordination between government agencies and their counterparts in neighboring countries and the world regarding ways to strengthen Yemen›s cybersecurity, according to Marib Press - March 2013.

Former Internet Society President Waleed al-Saggaf points out that one of the main challenges observed is the lack of sufficient skills on the part of technology users to keep their transactions safer and protect their websites and accounts, and the threats faced by Yemeni Internet users are a reflection of the risks associated with Internet use in general. World Watch on the Information Society - Previous source.

During the cyber extortion seminar last November organized by the Digital Rights Project, technical specialist Noor Khaled pointed out that companies, local institutions and international organizations in Yemen suffer from great technical laxity and negligence in following cybersecurity procedures, although any simple mistake can expose the institution, organization and company to breach and legal accountability.

It can be said that the division between the parties to the conflict in Yemen, and the state of polarization between regional and international actors, has damaged the Internet infrastructure in Yemen. According to a November 2018 report by Recorded Future, «Major international players, including the United States, Russia and China, are using malware, military activity, political influence and investments to advance their interests in the Saudi-Iranian regional struggle for dominance inside Yemen.

Threats and risks

-Censorship and external espionage

An October 2015 report by Citizen Lab (a laboratory that studies information controls that affect internet openness and security) stated that external and domestic electronic surveillance is widespread in Yemen, both before and during the current armed conflict.

The internationally recognized government has used China›s Huawei to help build its internet service provider. However, Huawei has been accused of using its technology to allow the Chinese government to spy on its customers. If this is the case in Yemen, it will pose a serious threat to the future of Yemeni cybersecurity. In fact, experts agree that both YemenNet and Aden Net are full of security vulnerabilities. According to the AGS program at Duke University - January 2018

Recorded Future expects there to be some Chinese monitoring of Yemeni activity, even if it›s just a way to monitor their investments. In addition, the fact that the Houthis control a vast amount of internet resources in Yemen, backed by Iran, and exercise de facto control over the country continues to antagonize the Saudi government, and this likely makes them a target for Saudi surveillance. Recorded Future expects this surveillance to be used primarily to determine Houthi intentions and combat plans for skirmishes across Yemen, targeting routers, traditional hosts and Android mobile devices. Recorded Future - November 2018.

In a serious incident, former NSA employee Edward Snowden revealed that the agency redirected YemenNet Internet traffic, and Yemeni communications as a whole, towards an NSA collection point, through a new, more convenient path for incoming traffic, by manipulating the BGP protocol on which the Global Internet Routing System is based.

Since it is difficult to intercept Yemen›s international communications from within Yemen itself, the agency has attempted to deliberately «shape» traffic to a more operationally convenient location for surveillance, passing through communications cables located in a friendly area, akin to turning part of the river into a site that is easier (or more legal) to fish, according to a study published by researcher Sharon Goldberg in The Center Foundation, in June 2017.

Although espionage and internal surveillance activities are outside the context of our report, we can refer to what leaked emails from the Italian spyware company Hacking Team showed that multiple requests were made from companies in Yemen seeking help in deploying surveillance tools in the country. In May 2013, more information was requested about Hacking Team›s Da Vinci interception system. Similarly, in March 2015, a client contacted the company asking for help, claiming to be the CEO of an IT security company that had a contract with Yemen›s National Security Agency «to develop systems, train and create a powerful tool to monitor, locate, and control Yemen›s overall communications range. However, it is not clear from the leaked email chains whether either company purchased Hacking Team products or services, and none of the scans conducted as part of Citizen Lab›s research on Hacking Team

and FinFisher showed evidence of control servers located in Yemen. Citizen Lab - October 2015.

-Malware attacks

Yemen ranked second among the top 10 countries and regions in terms of the percentage of users attacked by mobile malware, at a severity score of 18.91, out of 26, according to the report of the computer security company Kaspersky for the third quarter of this year 2022. The Trojan-Spy. AndroidOS.Agent.aas spyware was the threat that users often faced in the country. In addition, Yemen topped the list of countries where users were exposed to ransomware attacks via mobile devices, at a severity score (0.28%), and users in Yemen often encountered Trojan-Ransom.AndroidOS.Pigetrl.a.

Yemen also ranked second in the list of the top 10 countries and territories attacked by ransomware Trojans, on computers, with 1.30% of individual users whose computers were attacked by Trojan encryption programs (as a percentage of all individual users of Kaspersky products in the country), and fifth among the top 10 countries in the rate of exposure to financial malware attacks, with a rate of 2.3%. According to Kasper Sky›s report, for the third quarter of this year, Yemen ranked 11th in the list of countries where users faced the greatest risk of infection online, with an average of 12.58 users, and second among countries where users faced the highest risk of local infection (malware found directly on users› computers or removable media connected to them) with an average of 45.12% of users, an increase of 2% from the second quarter report.

According to the third quarter 2022 report issued by Avast (a Czech multinational cybersecurity software

company), users in Yemen were among the three countries most at risk of encountering the Remote Access Trojan (RATs), which extracts data from the infected computer, runs commands and code, and processes files on infected devices. Users in Yemen were also among the most at risk of information theft by Raccoon Stealer, which makes its way mainly to computers via «cracked» software, with a risk rate (+16%). Users in Yemen were also at higher risk of facing ransomware (0.53% risk) according to the report of the second half of the same year. Avast users from Yemen and four other countries also had the highest risk of exploit software, which exploits bugs and vulnerabilities in the system to execute malicious code remotely (RCE), according to Avast 2021. According to the Global PC Risk Report 2021, issued by Avast, Yemen ranked fourth among the ten countries most at risk of facing cyber threats in the Middle East and Africa, with an average of 46.21% of users of its services.

Yemen and Kenya accounted for the majority of victims of the Slingshot (Slingshot) program used for electronic espionage in the Middle East and Africa region from at least 2012 until February 2018. According to researchers at Kaspersky Lab, the program attacked victims with some lousy network routers, and then worked to collect screenshots, keyboard data, network data, passwords, USB connections, other desktop activities, clipboard and more. Kasper Sky - March 2018.

-Website piracy

The fact that Yemen is a relatively inexperienced country when it comes to internet-related technical operations has created a fertile environment for hacking websites, emails, and social media accounts, exploiting a lack of awareness of how technology works and how to take appropriate

precautions to prevent attacks during 2011-2012, according to a 2014 report by the World Information Society Watch Organization (GISWatch) (an organization that seeks to create an inclusive information society).

Cybersecurity expert Chris Plask noted in April 2013 that the risks of instability in Yemen resulting from cybercrime and cyberterrorism are real, and that many events highlight these risks, citing the hacking of TeleYemen, Yemen›s only international gateway, in the summer of 2012, which caused losses estimated at more than $20 million, according to Plask. In addition to what the Central Bank of Yemen suffered in the same year, where it suffered from many distributed denial-of-service attacks and its websites were infected several times with malware such as robots (Zeus Trojan). Chris Plask›s blog.

In November 2021, researchers at ESET (an IT security company, based in Bratislava, Slovakia) discovered strategic web hacking attacks linked to Candiru – an Israeli spyware company – against prominent sites in the Middle East, with a strong focus on Yemen, where the websites of the Ministry of Information and Saba News Agency were hacked, YemenNet, the websites of the Ministries of Interior and Finance, in addition to the websites of: (Yemeni Parliament, National Vision, Yemen Customs Authority, and Al-Masirah TV website), all under Houthi control, in Sana›a.

The attack was carried out using an «irrigation pit» that compromises websites that are likely to be visited by the targeted people, opening the door to an invasion of the site visitor›s device. In this campaign, it is possible that certain visitors to these sites have been attacked by browser exploitation.

However, ESET researchers were unable to obtain evidence of this exploitation, as the attackers only used the compromised sites as a stepping stone to reach the end targets.

-Phishing attacks via social media

Social media users in Yemen are subject to attacks aimed at hacking their personal accounts, either through social engineering [in which an attacker «uses human emotion to trick the target into doing an action, such as revealing authentication credentials,» according to the US digital security firm Proofpoint]. Or by clicking on malicious links, which are usually accompanied by tempting messages (such as getting help from an organization, cash prizes, internet credit... etc) or recording the account login details via false pages, created for this purpose.

For example, in a report published in October 2018, Post website revealed that the accounts of journalists on Twitter were hacked by parties that turned out to be operating from the capital, Sana›a, and hacked several Twitter accounts, most of which were known Yemeni journalists, by luring them with electronic tricks, reflecting in their entirety the existence of a network whose mission is to hack and acquire those accounts for the interests of those in charge of these operations.

A journalist received a message from an account called «Salah Khashoggi» advising him to verify his account with the blue tick by contacting the Arab Technical Support for Twitter through a WhatsApp number dedicated to this matter. The journalist followed these instructions via the WhatsApp number, an American number assigned to this trick, which is based on asking the victim for the email, password, and login data for the Twitter account, under the pretext of completing the verification process. Moments after the WhatsApp message, the account was hacked, the data

was replaced, and then the perpetrators of the operation corresponded with friends who follow the journalist and follow them on Twitter, most of whom are journalists. Some were defrauded in the same way after being contacted from the account of the journalist who was hacked, taking advantage of colleagues› trust in each other, and excluding their deception in this way.

Although phishing using free instant messaging programs such as Facebook Messenger or WhatsApp is not technically part of phishing, it is closely related, as the hacker exploits the increased level of comfort enjoyed by users by opening messages from strangers and responding to them through social media platforms. Trendmicro.

Ahmed Aslan, an expert in programming and information security, confirms that the purpose of those behind these phishing messages that spread randomly and reach unspecified users in chat groups on social media networks and privately, is their success in attracting the user and pushing him to click on the attached links to trap him in what he described as a trap, to then control his phone, which often leads to violent crimes and bullying that affect victims, taking multiple forms of threats, extortion and other electronic crimes. Website Post - July 2022

In June, the International Committee of the Red Cross (ICRC) in Yemen warned of unknown people sending misleading messages via WhatsApp containing fake information that the ICRC in Yemen is implementing an emergency program to help displaced and conflict-affected people obtain cash assistance. These fake and misleading messages ask people to access a suspicious app link to get the numbers of the alleged money orders. According to

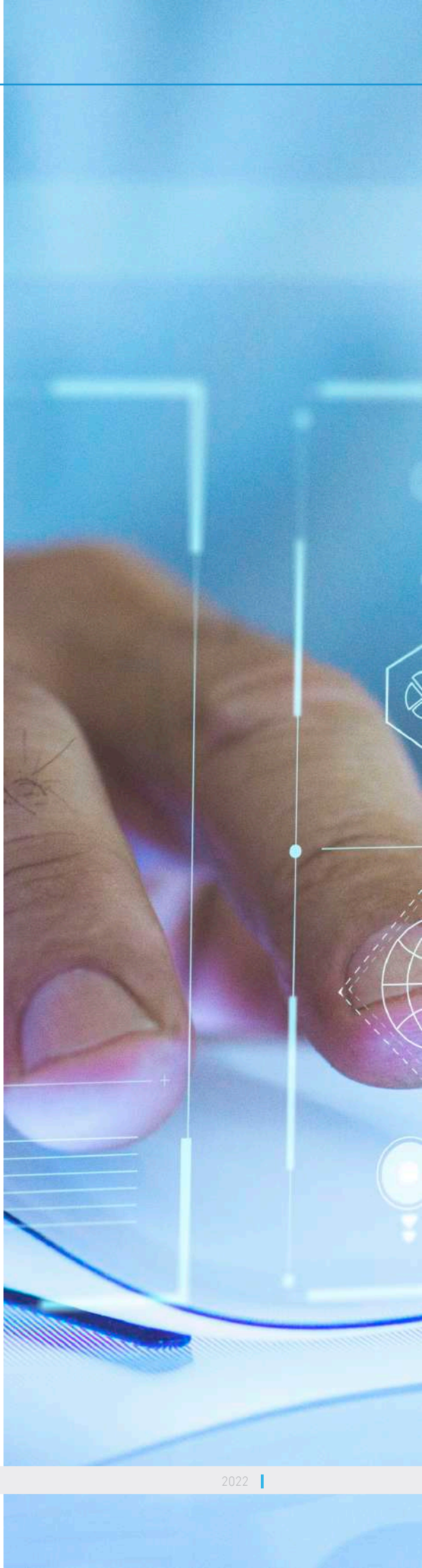
specialists, this may result in hacking the phones of those who install this application on their phones, putting their photos and personal data at risk.

It is noted that the application asks for the following permissions: access to the camera, files and media, call history, contacts, microphone, SIM messages, call management, geolocation, nearby devices) and if the application is installed, it means that the victim revealed his entire privacy, and exposed himself to danger.

-Applications and malware

Users in Yemen faced the highest risk of local infection (malware found directly on users› computers or removable media connected to them) with 45.12% of users, up 2% from the second quarter report. It is noteworthy that the company calculated the percentage of Kaspersky users on computers that have run Web Anti-Virus, and the classifications include only malicious object attacks that fall under the category of malware; they do not include Web Antivirus detections for potentially dangerous or unwanted programs. According to the KasperSky report, for the third quarter of this year.

In November 2018, Recorded Future noticed a significant increase in the number of software samples provided to VirusTotal from Yemen, from 13 samples between 2015 and 2017 to a total of 164 samples in 2018... Of these, almost half were malicious, and the vast majority of those malicious samples were Android apps. The company also noted the presence of several fake Altcoin altcoins and fake WhatsApp apps, spyware posing as antivirus, video drivers and VPN apps. Some samples of the AhMyth app, which allows smartphones to



be hacked and fully controlled, were connected to Chinese IP addresses. Two-thirds of counterfeit anti-virus spyware apps connected to Chinese IP addresses were found accessing information from Android phones including old emails, SMS, call logs and browser history. It will likely use accessibility services to control other installed apps and have the ability to change the Wi-Fi configuration and start services while the phone screen is off, as well as take photos and delete other packages. Recorded Future - November 2018.

Threat intelligence researcher at Recorded Future, Winona DeSombre, told CyberScoop in November 2018 that it is unclear whether the malware observed was used for either criminal or espionage purposes in Yemen. However, she said: «The intention of criminals to exploit people in a war zone, to carry out espionage... exists.»

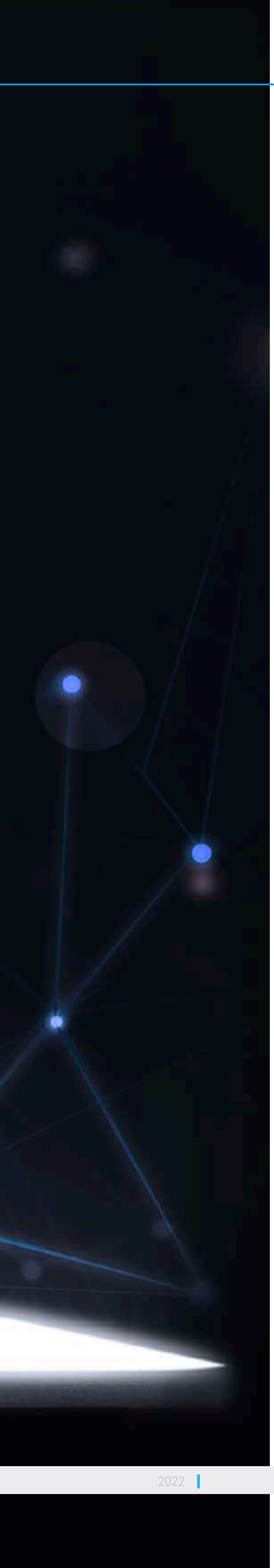
The volume of use of modified applications in Yemen, such as WhatsApp, for example, is increasing, which represents a real threat to users, as «the use of these clones is associated with potential security risks on the mobile phone and users› personal data. In addition, there is no way to ensure that these application files provide encryption for conversations or that sent messages do not pass through third-party servers before reaching the recipient, which may compromise security or even facilitate the leakage of personal and private information. Techidence October 2020.

What is the solution?

To enhance digital/information security in Yemen, former Internet Society President, academic Waleed Al-Saggaf, believes in a statement to the Digital Rights Project, that the focus should be on raising awareness among workers in the public and private sectors on how to identify and prevent cyber threats in their respective fields It is also important to develop and enforce strong cybersecurity laws and regulations, and to invest in advanced technology, especially open source that has been filtered from errors. Al-Saqqaf noted the importance of cooperation with international organizations and other countries such as the UAE, Oman and Jordan - because many cyber systems require Arabization - to learn from their experiences, especially in the field of education and the establishment of cyber service infrastructures.

Cybersecurity expert Chris Plask stresses the need to address cybersecurity by forming a Yemeni Cyber Emergency Response Team (Y-CERT) in order to mitigate the risks of cybercrime, cyberterrorism and economic decline. Having a strong cybersecurity infrastructure in Yemen could serve as a stepping stone for the country to address some of these challenges by employing Yemenis to address these cybersecurity issues, while bringing valuable additional benefits such as increased education and employment opportunities for citizens.

In a seminar organized by ITEX Technology on March 25, 2013, Engineer and IT expert Ali Al-Saghir Farhan called for the issuance of comprehensive laws, legislations and policies that regulate information security and criminalize cybercrime and the digital space, and stressed the need to educate people about cybersecurity, train judges, security and criminal research on how to detect information crimes and how to investigate them. He also called for the need to increase the sense of information security at the national level and at the level of individuals (especially users of the digital space). He stressed that the government›s responsibility towards cybersecurity is to train state employees, especially in the security and judicial sectors, to enforce the Digital Space Crimes Law and equip it to deal with cybercrimes. Marib Press - March 2013.



The participants in the First Information Security Conference (organized by the Public Telecommunication Corporation in cooperation with the International Telecommunication Union in June 2014) recommended the government to establish the Information Safety Center in Yemen (YE-CIRT) as a point of contact to respond to and address security problems and involve all relevant parties, with the need to prepare to build a national strategy to develop necessary solutions in the field of information security in cooperation with the International Telecommunication Union, and conducting a study to establish the Telecommunications Regulatory Authority and setting a general framework at the state level to fund information security requirements, and spreading community awareness in this regard through modern technology, through media programmes, educational curricula, conferences and workshops,. In addition to allocating a budget within the social responsibility of telecommunications companies, to sponsor and support information security awareness projects. They also called for the formation of a specialized preparatory committee to study the current laws in Yemen related to information security, and to compare similar laws in other countries to create laws and legislation to protect citizens and institutions. Al-Thawra Newspaper - June 2014.

At the individual level, technical specialist Noor Khaled noted during the electronic blackmail seminar last November organized by the Digital Rights Project the need for passwords to be strong and not to use any personal information, and to include a mixture of symbols and letters (Captl, Small), in addition to activating two-factor authentication via the Google Authenticator application. She stressed the importance of a person being very suspicious, so that he checks all the links received through social media platforms using the Virustotal website to ensure that they are malicious or safe. The technical specialist also warned against downloading any program from an unknown site, or installing modified applications such as Golden WhatsApp and WhatsApp Omar, because conversations will pass through a third party, in addition to making sure of the required permissions when installing any program or application, and if the required permissions are not related to the purpose of the application, it should not be installed.

Conclusion

The threats and violations against Internet users in Yemen are increasing, which calls for preventive measures at all levels (regulatory, legal, technical, technical... etc) The evolution of cybercriminal tactics requires institutions and individuals to keep pace with this development and follow the latest protection and security measures on the digital space.


سام
للحقوق والحريات

DIGITAL SECURITY IN YEMEN. REALITY AND THREATS

December 2022

violations@samrl.org
www.dg.samrl.org

Digital.Rights.Yemen
@SamDigitalRight

SAM Rights & Liberties

www.samrl.org
info@samrl.org