MALWARE TREND REPORT

To educate and improve awareness, preparedness and readiness in facing cyber threats

H2 2019

July - December 2019

TABLE OF CONTENT

DISCLAIMER

This document is for informational purposes only. Every effort has been made to make this document as complete as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. CyberSecurity Malaysia, the Permanent Secretariat of the Organisation of the Islamic Cooperation – Computer Emergency Response Team **(OIC-CERT)**, shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Information on the malware trend is made available by CyberSecurity Malaysia for the purposes of providing awareness and improving the preparedness and readiness in facing malware threats.

The logo and names of organisations and products mentioned herein are the trademarks of their respective owners. The use of the logo and name do not imply any affiliation with or endorsement by the respective organisations.

THE OIC-CERT MALWARE TREND REPORT H2 2019

The OIC-CERT Malware Trend Report is a series of reports produced half yearly for the Malware Research and Coordination Facility Project (the Project). The Project is a collaborative effort of the Organisation of the Islamic Cooperation – Computer Emergency Response Team **(OIC-CERT),** the Asia Pacific Computer Emergency Response Team **(APCERT)** and other organisations from various countries. The Project is an initiative by CyberSecurity Malaysia as the Permanent Secretariat of the OIC-CERT. The background of the Project and the participating agencies / organisations is listed in "About the Project" section at the end of this report.

This Malware Trend Report published covering the period of 1 July 2019 until 31 December 2019.

INTRODUCTION

The Fourth Industrial Revolution **(IR 4.0)** is a new revolution that is set to transform the technology landscape. The premise of Industry 4.0 is all about the integration of physical and digital technologies [1]. With the infusion of the 5G network, short for fifth-generation wireless, IR 4.0 promises to be the heartbeat of the future which able to provide smart, connected technologies and becoming mainstream in manufacturing where manufacturers can use connected systems to gain critical insights about their operations.

The 5G technology is set to be embedded in so many fields of endeavour, the country that dominates the technology is likely to reap outsize profits, attract top-tier engineering talent and seize an edge in other critical future technologies, including weaponry [2]. Due to its capability, 5G becoming the race between world's largest economy. For political purposes, that "race" has been defined as which nation gets 5G built first.

Every new technology seems to bring with it some new vulnerability for its users. Because of the vulnerabilities of software, the tougher part of the real 5G "race" is to retool how we secure the most important network in the 21st century and the ecosystem of devices and applications that emerge from that network [3]. It is essential for enterprises to improve their security measures by using full-spectrum security that protects the whole infrastructure of the business from being negatively impacted by the cyber threats [4] as 5G has challenged the traditional assumptions about network security concept.

OBJECTIVES

This report aims to provide a better understanding of the malware threats and analysis as well as the related potential impacts mainly within the participants' community. The objective is to educate and improve awareness, preparedness, and readiness in facing cyber threats.

TARGET AUDIENCE

The malware threat analysis presented in this report is primarily for the consumption of the Project participants and the general Internet users.

TOP ATTACK TYPE

A cyberattack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually, the attacker seeks some type of benefit from disrupting the victim's network. The attack can be in any possible medium such as using malware, phishing, man-in-the-middle attack (MitM), denial-of-service attack (DDoS) or SQL injection.

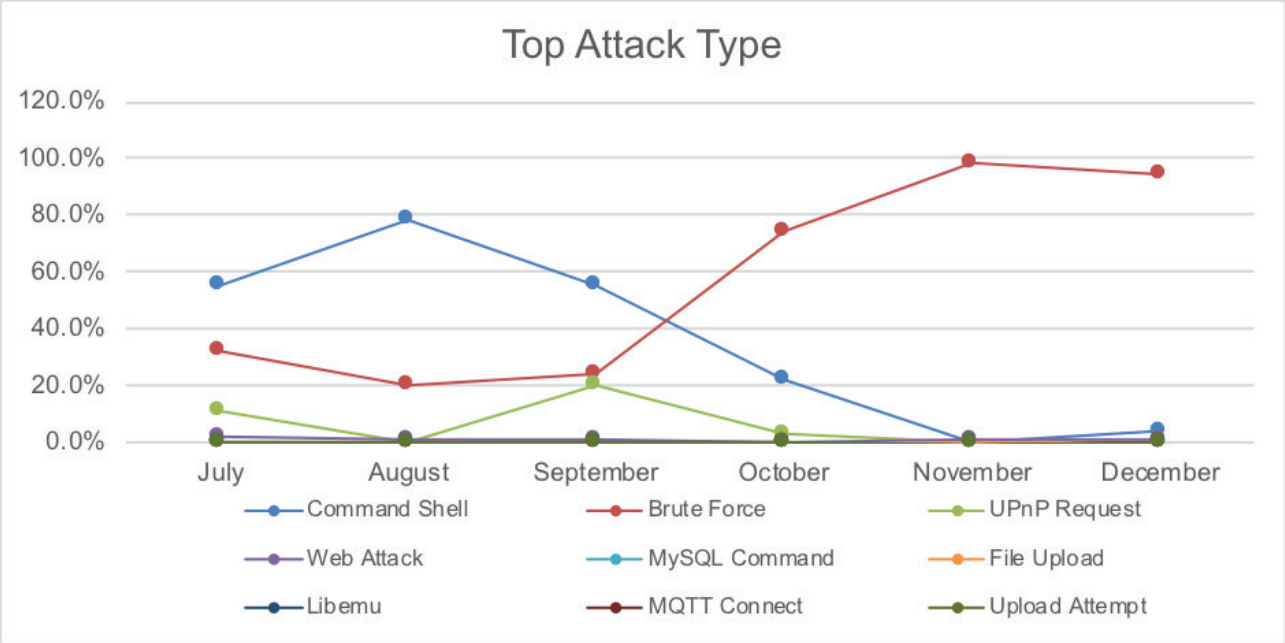

Figure 1 : Top Attack Type

Figure 1 above illustrates the statistics of top attack types logged for the Project from January to June 2019. Based on Figure 1, Brute Force attack recorded as the highest attack for four months but dropping for March and April while UPnP attack showing an increase in April. MQTT Connect also showing an increase in March. Figure 1 also indicate that the pattern of SSH Banner attack is slightly the same with Brute Force attack but with smaller percentage.

THREAT ORIGIN (TOP 10)

The threat origin refers to the malicious traffic by country. However, the attacker may not necessarily stay in the same country where the traffic is sent. The vulnerabilities of the servers at the country of origin are probably being utilised by the attackers as a part of the attack mechanism. The countries that are placed at the top maybe due to the availability of robust networks and volume of devices within its borders which are suitable for the attackers modus operandi. For malicious traffic by country of origin, the data is broken by month as below.

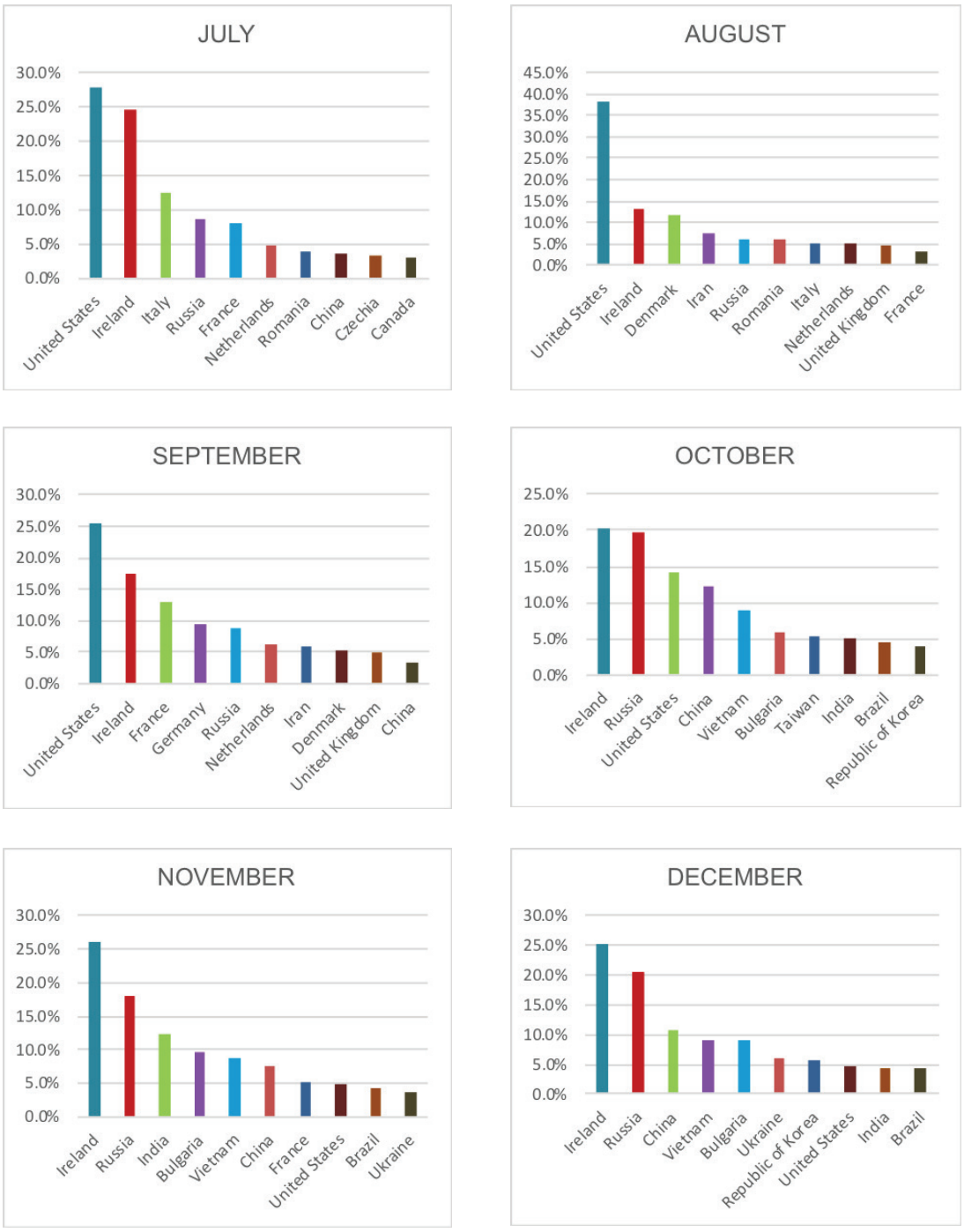

Figure 2 : Threat Origin

Figure 2 shows the top 10 of origin of threats for each month from July to December 2019. As stated before, kindly note again that the attacker may not be in the same country where the traffic is sent as the attacker may be using infrastructure in the country to launch the attack.

TARGETED SERVICES

The computer network technology is developing rapidly, and the development of internet technology is more quickly, people more aware of the importance of the network security. Network security is main issue of computing because the attacker today is utilizing the network services to gain access to the targeted organisation.

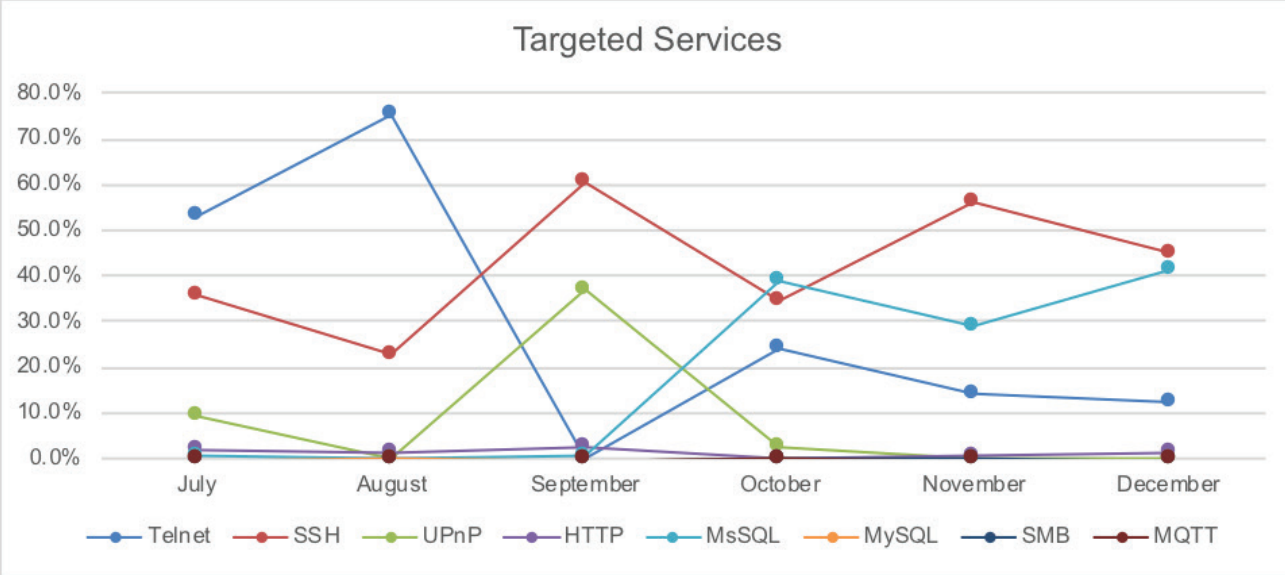

Figure 3: Overview of the targeted network services

In Figure 3, eight (8) targeted services data are logged during the H2 2019 period. It is observed that the attack count is different from one month to another. As example for Telnet services; the attack is decreasing sharply in September then showing slight increase in October. Figure 3 also demonstrating that SSH is attacked is fluttered but that quite high rate.

RANSOMWARE

Since the global pandemic in May 2017 [5], ransomware strikes are getting bolder [6] . Due to its potential, ransomware has been commoditised as a service in the cybercrime community [7]. Based on the ransomware evolution trends, experts does not see an end to ransomware anytime in the near future [8] but anticipated the ransomware to make further rounds [9].

The predictions proved that the ransomware is not only targeting profitable companies [6] but also the government. In July 2019, two (2) local agencies in Georgia have been hit with ransomware attack. The Henry County government was struck by a similar ransomware attack on July 17, while the Lawrenceville Police Department was hit on July 19 [10]–[13].

As for this project, specifically during this period of data from July until December 2019, only one (1) type of ransomware was detected which is WannaCry ransomware with total of 460 unique hashes.

TOP 10 PASSWORD

The worst passwords tend to be the most hacked, simply because they are way too easy to crack. So, it should come as no surprise that the bad passwords report from SplashData password management firm, have indicated the same. SplashData releases its annual list as an effort to encourage the adoption of stronger passwords. In its ninth annual Worst Passwords List, SplashData looked at more than 5 million passwords that were leaked online [14].

The Project is also captured the password used by attackers. The results below list the regularly used passwords in attempt to breach the system to access sensitive information.

Password	Percentage (%)
admin	50.4
ubnt	19.9
{blank}	17.9
system\x00	4.5
sh\x00	4.1
123456	0.9
/bin/busybox SELFREPPING\x00	0.9
12345	0.6
1234	0.5

Table 1: Top 10 Password

admin (50.4%) is the most common used password in attempt to access the targeted system followed by ubnt (19.9%) password. 3 from top 10 password captured in this Project are listed in SplashData list [14]. They are admin, 123456 and 12345.

CONCLUSION

Cybercriminals will go after any business that allows for a quick attack and quick return. It is important to remember that the cyber-attack is still a real, present threat for your organisation regardless of the size [15], [16]. If a small and medium-sized enterprise (SME) is being attacked, the business is doubly susceptible to financial losses as not only it will incur remedial cost after being hit by hackers and other cyber criminals, but the company also risk losing customer confidence that will hurt sales figure.

Apart from setting up the required elements in protecting the cyber security, the organisations should also educate the employees with the basic information of cyber security as majority of breaches are due to insiders [17]. Educating the employees could help in preventing them from making the business vulnerable to cyber-attacks [18].

ABOUT THE PROJECT

Background

The Malware Research and Coordination Facility Project was initiated by CyberSecurity Malaysia, whom is also the Permanent Secretariat of the OIC-CERT. The participating agencies / organisations subscribing to this Project share malware data that allow collective malware threat analysis to be done. Such analysis provides early detection of malware for the corresponding advisories to be provided. The analysis and recommendations allow government and organisations to react against the malware threats and protecting their assets against the detrimental effect of malware infection which typically leads to cyber-attacks.

Table 2 list the agencies and organisations that are participating in the Project. The services of the Malware Research and Coordination Facility are also offered to the members of the Asia Pacific Computer Emergency Response Team (APCERT) and the APCERT Malware Mitigation Working Group based on the Memorandum of Understanding (MoU) between the OIC-CERT and APCERT.

The participating agencies / organisations in the Project are:

Country	Percentage (%)
Bangladesh	1. Bangladesh Computer Emergency Response Team (bdCERT) 2. Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)
France	Alliacom
India	Indian Computer Emergency Response Team (CERT-In)
Japan	Japan Computer Emergency Response Team / Coordination Center (JPCERT/CC)
Malaysia	1. AIMS 2. Politeknik Mersing Johor 3. Telekom Malaysia 4. Universiti Malaya 5. Universiti Teknikal Malaysia Melaka
Nigeria	Ibrahim Badamasi Babangida University
Philippines	Cyber Security Philippines Computer Emergency Response Team (CSP-CERT)
Taiwan	Taiwan National Computer Emergency Response Team (TWNCERT)

Table 2 : List of participating countries and organisations

Data Source

The data, information and analysis used to produce this Malware Trend Report H2 2019 are derived from the malware data generated by various sources within CyberSecurity Malaysia and the participating agencies / organisations in this Project such as:

- Network security devices (active and passive) installed regionally;
- Managed security services; and
- User reported cases.

Top 50 Malware Hash

Below are lists of hashes of the files which contain malware detected in this Project:

a52e5c9d39889647a84d00361954f3fe47685d0af63dfc28e3664ccea60ef600	
ae12bb54af31227017feffd9598a6f5e	44ade454a487822f1c9d75aa7d8df907
cd3827f2a3e24e472d217acccd51dcdef44ee756c47f9fb0e369d64d44cf2246	
34bec532c7a529a9b2e0626d237bab3f	3062df26ec61ca773e8c7cd487322562
58501baa508d8609f2a91652634271aa6bfbe6a599db60632aafc6c0d85eb576	
996c2b2ca30180129c69352a3a3515e4	414a3594e4a822cfb97a4326e185f620
0ab2aeda90221832167e5127332dd702	add63c406aefbb2b2fa66a92d1576d62
b47c98f2421929093b268e38c9d4559f	6e72ad805b4322612b9c9c7673a45635
fae1c9a6cafcdf299f86a78ffed4e371b82b05b3f09eb933d866ab3244d0c704	
01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b	
e9d1ba0ee54fcdf37cf458cd3209c9f3	033f9150e241e7accecb60d849481871
61545c33f327d15b80f0d251a67d1a8d	474ecb2fac7ef6f1b798d81d8a3ba5a2
474ecb2fac7ef6f1b798d81d8a3ba5a2	09bddc28576dc82a4f9e2b350d617fc6
ff6f81930943c96a37d7741cd547ad90295a9bd63b6194b2a834a1d32bc8f85d	
95ae8e32eb8635e7eabe14ffbfaa777b	d195c8f601061342db3ae15c539878ac
a55b9addb2447db1882a3ae995a70151	99f11e1759e82983cb0d12118eadfa03
719b5b77b91d45e98d4891f0914fa3072b50cdc58c3569a07b06ea39c65562c3	

ce494e90f5ba942a3f1c0fe557e598bf	832e5d2338f375cd669e65fde70cb6db
bd80975a347bc35121202a0a8c443ed7dcc7f635d1c6d0159236963c30daa12a	
1b0afa339f844c523fee007a9bea6e3c3c38658997ce6ead1ea8490c1f9c82ac	
abe895661991e7520e3ed407e65190155305d3327f754e79f7dda54da0da1a1a	
cf4f46336abeec03630297f846d17482	685bc2af410d86a742b59b96d116a7d9
8e6bfea06cb00553ee29b3822b349bd6	52fbcf95ee0747a5482185096fab8468
a944604a17c71d2a3243fd084598f45c	7867de13bf22a7f3e3559044053e33e7
786ab61623981461664 2ba4438df78a9	cd99e5e4f44621978faf8df0e01d2d2b
ed258755f3ad40edfcad2dcccfd7cde04ab38ef159b0b84577a480cec9d7e325	
9aa3637857d84aa040c097ba0be6b900	e92132738a3e4fd1881a4b8a6901988d
7ca054f079f297dd6462630cd5009aa7510a5b21290d9a9fbf8ef72da07b3e6f	
01bdc6fb077098f4a3b60f4b0e479a7f	235e9af4c6f5b5de7d30d0589bbcff14
4355a46b19d348dc2f57c046f8ef63d4538ebb936000f3c9ee954a27460dd865	
a4d49eaf60a8e333708469606ad9e1a4	35a952b9fac6df9c1e0463f4d4b15023
f70557802f671ae027d602d2bd3fd6cf	

ADVISORY

The LebahNet sensors have managed to capture varieties of malware. Below are some of the recommendations in preventing malware infections.

- Always keep the patches up to date (if possible, using virtual patching solutions), especially on computers hosting public services and are accessible through firewalls such as HTTP, FTP, mail, and DNS services.
- Ensure that all the latest patches are applied to the affected operating systems – especially those related to MS17-010.
- Proactively monitor and validate traffic going in and out of the network.
- Implement security mechanisms at other points of entry which the attackers can use, such as email and websites.
- Deploy application controls to prevent suspicious files from executing, in addition to behaviour monitoring, that can thwart unwanted modifications to the system.
- Implement data categorization and network segmentation to mitigate further exposure and damage to the data.
- Disable SMB(v1) on vulnerable machines – using either GPO or by following the instructions provided by Microsoft.
- Do not click suspicious hyperlinks and do not open mature photos or videos received from social networks or instant communications.
- Switch on the system restore features of the operating systems.
- Deactivate the Windows PowerShell construction and Windows Script Host (WSH) technology.
- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- Enforce the password policy. Complex passwords make it difficult to access files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Ensure that the programs and users of the computers use the lowest level of

privileges necessary to complete their task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.

- Disable the AutoPlay to prevent the automatic launching of executable files on the network and removable drives and disconnect the drives when they are not required. If write access is not required, enable read-only mode if the option is available.
- Turn off the file sharing function if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues for cyber attacks. If they are removed, there will be less vulnerabilities thus reducing threats and attacks.
- If a threat exploits one or more network services, disable or block the access to the services until required patch is applied.
- Configure the email servers to block or remove emails that contains file attachments that are commonly used to spread threats such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers immediately to prevent threats from spreading. Perform a forensic analysis and restore the computers using trusted media.
- Train the employees not to open attachments unless they are from a trustworthy source. Do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Visiting a compromised website can cause infection if certain browser vulnerabilities are not patched.
- If Bluetooth connection is not required for mobile devices, it should be turned off. If it is required, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be done, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.

REFERENCES

[1] A. Ross, "Why 5G is the heart of Industry 4.0," 2019. [Online]. Available: https://www.information-age.com/5g-is-the-heart-of-industry-4-0-123483152/. [Accessed: 14-Jan-2020].

[2] S. Woo, "In the race to dominate 5G, China sprints ahead," 2019. [Online]. Available: https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888. [Accessed: 14-Jan-2020].

[3] T. Wheeler and D. Simpson, "Why 5G requires new approaches to cybersecurity," 2019. [Online]. Available: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/. [Accessed: 14-Jan-2020].

[4] R. Sens, "Be ready to fight new 5G vulnerabilities," Netw. Secur., vol. 2018, no. 10, pp. 6–7, 2018.

[5] Symantec Security Response, "What you need to know about the WannaCry Ransomware," 2017. [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack. [Accessed: 14-Jan-2020].

[6] AFP, "Ransomware attacks 'getting bolder': Europol," 2019. [Online]. Available: https://www.thestar.com.my/tech/tech-news/2019/10/10/ransomware-attacks-getting-bolder-europol. [Accessed: 14-Jan-2020].

[7] S. Mansfield-Devine, "Ransomware: the most popular form of attack," Comput. Fraud Secur., vol. 2017, no. 10, pp. 15–20, 2017.

[8] Trend Micro, "The evolution of ransomware," 2018. [Online]. Available: https://blog.trendmicro.com/the-evolution-of-ransomware/. [Accessed: 14-Jan-2020].

[9] Trend Micro, "Security predictions for 2018," 2017. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018?_ga=2.205296784.1618499482.1578979959-1425711309.1578979959. [Accessed: 14-Jan-2020].

[10] NNT, "Country of Georgia hit by widespread cyber attack," 2019. [Online]. Available: https://www.newnettechnologies.com/country-of-georgia-hit-by-widespread-cyber-attack.html. [Accessed: 14-Jan-2020].

[11] BBC News, "Georgia hit by massive cyber-attack," 2019. [Online]. Available: https://www.bbc.com/news/technology-50207192. [Accessed: 14-Jan-2020].

[12] L. Ropek, "Georgia Public Safety Agency hit with ransomware attack," 2019. [Online]. Available: https://www.govtech.com/security/Georgia-Public-Safety-Agency-Hit-with-Ransomware-Attack.html. [Accessed: 14-Jan-2020].

[13] S. Thanawala, "Georgia county ransomware attack highlights cyber exposures to local agencies," 2019. [Online]. Available: https://www.insurancejournal.com/news/southeast/2019/10/23/546298.htm. [Accessed: 14-Jan-2020].

[14] SplashData, "The top 50 worst passwords of 2019." [Online]. Available: https://www.teamsid.com/1-50-worst-passwords-2019/. [Accessed: 05-Jan-2020].

[15] "SMEs are doubly at risk of losing to cyber crime," 2017. [Online]. Available: https://cxloyalty.co.uk/news-resources/smes-risk-cyber-crime/. [Accessed: 14-Jan-2020].

[16] A. Jalil and M. A. Naharul, "84% of SMEs fell victim to cyber attack last year," 2019. [Online]. Available: https://themalaysianreserve.com/2019/10/17/84-of-smes-fell-victim-to-cyber-attack-last-year/. [Accessed: 14-Jan-2020].

[17] Verizon, "2019 data breach investigations report," 2019.

[18] Infosec, "Security awareness -- Definition, history, and types." [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/securityawareness/#gref. [Accessed: 14-Jan-2020].

OIC-CERT Permanent Secretariat:
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.

secretariat@oic-cert.org
www.oic-cert.org