MALWARE TREND REPORT

H1 2019 January - June 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 H1 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 January 2019 until 30 June 2019.

INTRODUCTION

Malware trend in half 2019 continues showing of grow on cybercriminals. Threat actors consistently improved their cyber weapons and quickly adopted new methods and adapted their attacks to emerging technologies. Although it may have seemed the past year was quieter, this is far from the case. While threat actors were trying hard to keep a lower profile with their menacing activities, they could not escape our watchful eye. Indeed, there is no single day passed by without cyber incidents. The Q4 Threat Report by Fortinet has highlighted the critical need of threat intelligence to protect an organisation [1].

In January, Singapore's Ministry of Health (MOH) revealed a data breach involving 14,200 individuals. While the number may not seem all that serious, MOH has ascertained that confidential information regarding 14,200 individuals diagnosed with HIV up to January 2013, and 2,400 of their contacts, is in the possession of an unauthorised person [2].

April this year, a security firm has found detailed information about more than 540 million Facebook users were left publicly viewable for months. Two Amazon Web Services (AWS) servers were found by researchers to store the records including account names, Facebook IDs, and user interaction data [3], [4]. The servers in question were owned by third parties and were not properly secured.

Data breaches occurrences does not only threaten the related government information infrastructure, but also third-party services. The saying "there is no such thing as bad publicity" may portray the effect of the incident where the customers will think of the incident as a violation of trust.

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

Cyber attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer device; using various methods to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin privileges on it.

Based on history of famous battles, none of their battle tactics is exactly alike. Still, there are similarities between the strategies and tactics often used as they are time-proven to be effective. Similar to cyber attacks, when an attacker is trying to gain access to an organization, they will not invent new wheel unless they absolutely have to do it. The attacker will draw upon common types of hacking techniques that are known to be highly effective.

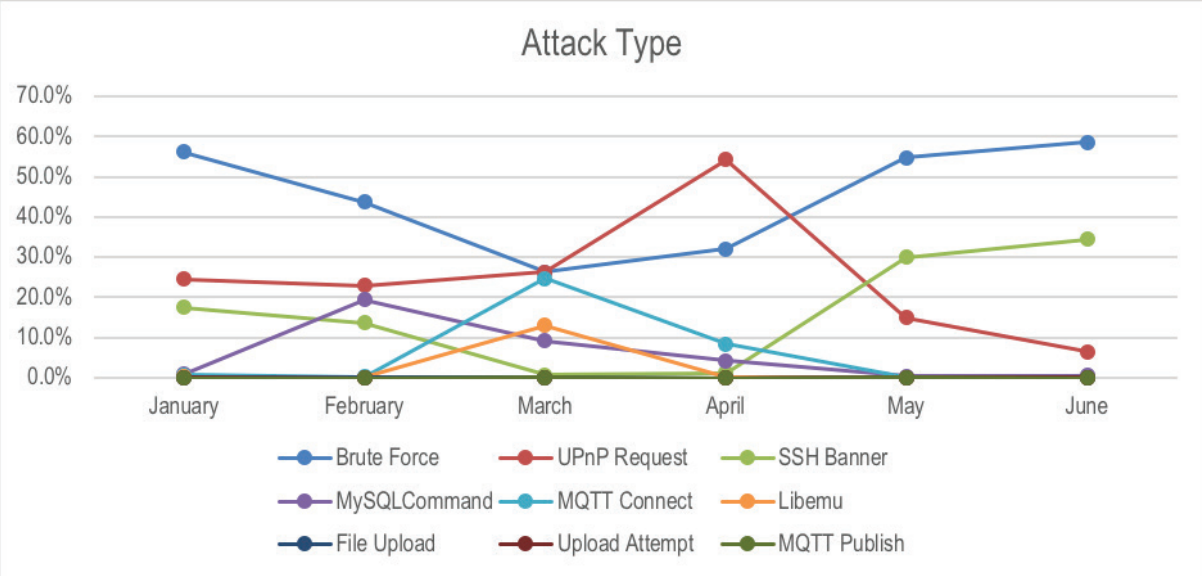

Figure 1 : Top Attack Type

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 necessary stay in the same country where the traffic is sent. The origin of the attack is driven by the mechanisms available to the bad actor. The country that placed at the top maybe due to the robust networks and volume of devices within its borders. For malicious traffic by country of origin, the data is broken by month as below.

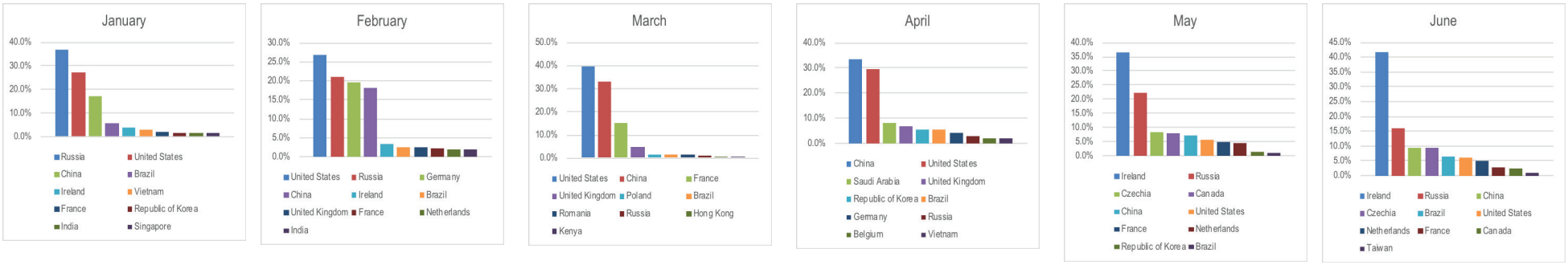

Figure 2 : Threat Origin

Figure 2 shows the top 10 of origin of threats for each month from January to June 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 organization.

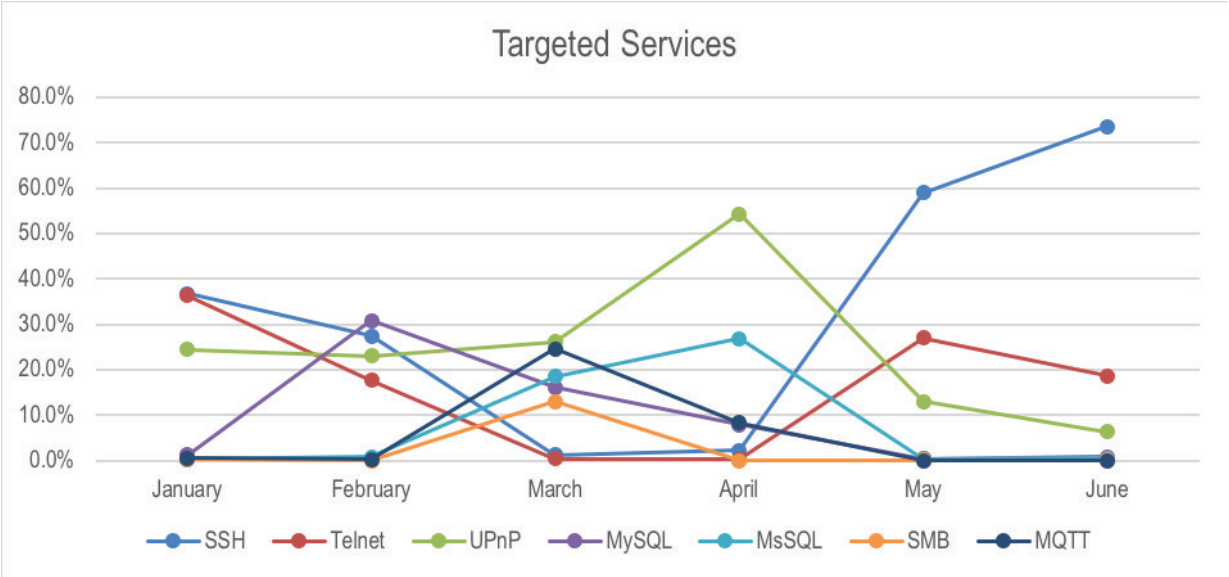

Figure 3: Overview of the targeted network services

In Figure 3, seven (7) targeted services data are logged during the H1 2019 period. It is observed that the attack count is different from one month to another. As example for SSH services; the attack is decreasing from January to March, then slight increase in April and shot up in May. This result shows that the cyber attack trends are unpredictable.

RANSOMWARE

During this period of data from January until June 2019, only one (1) type of ransomware was detected which is WannaCry ransomware. In fact, the WannaCry ransomware is still active since 2017 till now. After two years of attacked which cost the National Health Service almost £100m and led to the cancellation of 19,000 appointments, the epidemic ransomware, WannaCry is still not fading away, which responsible for 28.72% of ransomware attacks in Q3 2018 [5], [6].

Despite these very real threats, ransomware has been in declined over 2018 and 2019. The drop was steep: ransomware affected about 48 percent of organizations in 2017, but only 4 percent in 2018 [7].

TOP 10 PASSWORD

Humans are the weakest cybersecurity link. One of the factors contributing to the cyber attack is the use of weak password, especially when it comes to privileged accounts, such as local or domain administrator users. The UK's National Cyber Security Centre (NCSC) 'UK cyber survey' published in April 2019 listed the global password risk list [8].

That was the unsurprising conclusion of a survey revealing the internet's most vulnerable passwords, which also warned that codes using names, sports teams and swear words are more popular than you might think. Several combinations of numbers made up the top 10, while "blink182" was the most popular musical artist and "superman" the most common fictional character.

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	25.08
{blank}	14.82
ubnt	10.56
1qaz2wsx	6.09
password	6.02
system\x00	5.00
sh\x00	4.40
12345678	3.20
12345	2.81

Table 1: Top 10 Password

admin (25.08%) is the most common used password in attempt to access the targeted system followed by {blank} (14.82%) password. Top 10 of top used password made up 77.99 per cent where the other password is 22.01 per cent.

CONCLUSION

As we have seen, the recent attacks are being more focused on and developing new threats to leverage additional entryways. Regardless of whether completed by individuals or country expresses, these attacks uncover interesting new patterns and motivations. From cryptomining, ransomware to IoT vulnerabilities, every single occurrence made a significant impact on today's threat landscape.

This report can make a significant difference to the parties' ability to understand better the facts and would useful to everyone involved in decision-making. Although it is difficult to be fully prepared for any incoming threat, having threat intelligence and regular audit are essential for an organisation in order to eradicate and remediate any threats.

Furthermore, it provides insight for both strategic direction and areas to address technically.

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)
China	National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT)
France	Alliacom
India	Indian Computer Emergency Response Team (CERT-In)
Japan	Japan Computer Emergency Response Team / Coordination Center (JPCERT/CC)
Malaysia	1. University Teknikal Malaysia Melaka 2. Telekom Malaysia 3. AIMS 4. University Malaya
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 H1 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:

ae12bb54af31227017feffd9598a6f5e
44ade454a487822f1c9d75aa7d8df907
474ecb2fac7ef6f1b798d81d8a3ba5a2
0ab2aeda90221832167e5127332dd702
996c2b2ca30180129c69352a3a3515e4
6e72ad805b4322612b9c9c7673a45635
add63c406aefbb2b2fa66a92d1576d62
e9d1ba0ee54fcdf37cf458cd3209c9f3
414a3594e4a822cfb97a4326e185f620
ca71f8a79f8ed255bf03679504813c6a
a55b9addb2447db1882a3ae995a70151
f39a5dcc9ee715862461b54f2cc1c837
95ae8e32eb8635e7eabe14ffbfaa777b
033f9150e241e7accecb60d849481871
9aa3637857d84aa040c097ba0be6b900
1f80e75bc4168a96c52754570925179 8
8e6bfea06cb00553ee29b3822b349bd6
3860bdea429da898e48421ae950340ee
294280cfdcfdce1b14d25d7a51a2a228
dc987c107275c54d7af47b28d1908693
52fbcf95ee0747a5482185096fab8468
832e5d2338f375cd669e65fde70cb6db
235e9af4c6f5b5de7d30d0589bbcff14
62eceac3e1b568a8f807de6c9b15590e
35a952b9fac6df9c1e0463f4d4b15023
7867de13bf22a7f3e3559044053e33e7
60ad1b61d6a6a9c6313ac3da13954b43
3695f6d3175e85e25ea3cc65ab3801cf
8c81ab1ed40c6a1b1d359b305c1c8d7d
cf4f46336abeec03630297f846d17482
f082f12f9dbc67f7c42c8db4b126835f
cd99e5e4f44621978faf8df0e01d2d2b
b18487f13fbaf411aaedd699a56e5a6d
f647420c0fe55b1cee853600d60feb14
51d00ac16ce607d29fd7c1c4cc953cdf
cbd91d483bc5d87b16938163e75ef67f
74bc261ad11bc9f1d57641998dc1fe69
a3e21eaf099d33e5c82062e46ffc537b
8831cfc4b15416f07eb34d944641e179
cc435ef3d7e00bcb2720743f17705323
c495c1b70e41b42753c098dec2ef5af3
879d69d4c18d6947f9ea5e545ac16d01
f974b44ec540321c7125866d0fe3d18c

ab2044c2e74bd1a6518a75c6bdf17c6f
1d44fb198c3676f4f71bbac33075294c
99cd95db92c4e4cb4b882eb034e75cab
24899e33d1f6f7d1dbb4ecb458c4f057
9a906134786ad70fa5569049189200ae
ed979ce49b3373765a91b15c1c37c00b
3ce7baba17fcf32f7310e9ab435b9511

REFERENCES

[1] J. Jarvis, "Q4 threat report: 2018 attacks highlighted the need for advanced threat intelligence," *Fortinet*, 2019. [Online]. Available: https://www.fortinet.com/blog/industry-trends/q4-threat-landscape-report--2018-attacks-highlighted-the-need-fo.html. [Accessed: 06-Jul-2019].

[2] Ministry of Health Singapore, "Unauthorised possession and disclosure of information from HIV registry," *Ministry of Health Singapore*, 2019. [Online]. Available: https://www.moh.gov.sg/news-highlights/details/unauthorised-possession-and-disclosure-of-information-from-hiv-registry. [Accessed: 07-Jul-2019].

[3] BBC, "Data on 540 million Facebook users exposed," *BBC News*, 2019. [Online]. Available: https://www.bbc.com/news/technology-47812470. [Accessed: 10-Jul-2019].

[4] M. Murphy, "Millions of Facebook user records exposed in data breach," *The Telegraph*, 2019. [Online]. Available: https://www.telegraph.co.uk/technology/2019/04/03/millions-facebook-user-records-exposed-data-breach/. [Accessed: 10-Jul-2019].

[5] V. Chebyshev, F. Sinitsyn, D. Parinov, O. Kupreev, E. Lopatin, and A. Liskin, "IT threat evolution Q3 2018. statistics," *Kaspersky Lab*, 2018. [Online]. Available: https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/. [Accessed: 02-Jan-2019].

[6] M. Field, "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled," *The Telegraph*, 2018. [Online]. Available: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/. [Accessed: 07-Jul-2019].

[7] W. Ashford, "Ransomware in decline, report confirms," *ComputerWeekly.com*, 2019. [Online]. Available: https://www.computerweekly.com/news/252456240/Ransomware-in-decline-report-confirms. [Accessed: 10-Jul-2019].

[8] NCSC, "UK cyber survey key findings," 2019.

If you have any enquiries or comments about the Malware Trend Report or you would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone or email:

CyberSecurity MALAYSIA

The Permanent Secretariat of the
Organisation of the Islamic Cooperation –
Computer Emergency Response Team (**OIC-CERT**)

Level 7, Tower 1, Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan

+603 8800 7999
international@cybersecurity.my
secretariat@oic-cert.org