ISKO Information Security

First 100 days of COVID

MAY 2020

Cordev

COVID-19 has provided many new opportunities for cyber threat

As staff are working from home, there has been a measurable increases in spam and impersonation attack campaigns.

Threat categories	January to end of March 2020
Spam/ opportunistic detections	increased by 26.3%
Impersonation detections	increased by 30.3%
Malware detections	increased by 35.16%
Blocking of URL clicks	increased by 55.8%

Source : www.mimec

NITED

STAY HEALTHY,
STAY CYBER-SAFE

AIL EXTORTION CAMS

HOW THE SCAM WORKS

1. You receive an email claiming that your device/account has been compromised
2. Scammer claims to have your 'private and confidential' information
3. A ransom is demanded to keep the information private
4. Scammer may use your email and password from past data breaches as 'proof' that the email is legitimate

WHAT SHOULD YOU DO?

Do not make payment. Delete the email immediately.
To prevent unauthorised access, you should:

rong passwords
t are long and
random

Do not use personal information (e.g. NRIC) in your passwords

Use different passwords for different accounts

ble Two-Factor
entication (2FA)
ben available

Perform anti-virus scans on all devices

Keep your software up-to-date

If you wish to provide any information related to such scams, please call the Police hotline at 1800-255-0000 or submit it online at www.police.gov.sg/iwitness.

SG UNITED

STAY HEALTHY,
STAY CYBER-SAFE

USING ZOOM?

STAY CYBER-SAFE WITH THESE TIPS

1 Use the Latest Zoom Application

Download the app from the official website and install updates immediately when available.

2 Secure Your Meeting

Require registration, password access and generate a unique ID for meetings. Do share ID and password with intended participants only. Use a strong password.

3 Manage Meeting Access

Enable the waiting room feature, disable 'join before host' option and remove any unknown participants. Lock the meeting once everyone has joined.

4 Control Meeting Functions

Set sharing screen to 'host only' and disable private chats. For audio-only meetings, disable video calls.

5 Safeguard Sensitive Info

Do not share sensitive files or hold sensitive discussions. Only enable file sharing and meeting recordings if needed.

6 Be Alert for Phishing Attacks

Avoid clicking on suspicious links and attachments in the chat function.

7 Update Your Devices

Ensure that the OS and anti-virus software of the device(s) installed with Zoom are updated.

WANT TO LEARN MORE?
Visit www.csa.gov.sg

SG UNITED

STAY HEA
STAY CYBER

IMPLEMENTING A REMOTE WORK POLICY? STAY CYBER-SAFE WITH THESE TIPS

1. Stay Updated

Update all VPN, network infrastructure and endpoint devices to the latest patches

2. Set Authentication

Enable Multi-factor Authentication for all VPN connections

3. Secure Your Systems

Follow good practices guides recommended by solution providers

4. Audit Regularly

Check privileged domain and local system accounts routinely to detect unknown accounts

5. Spread Awareness

Provide regular reminde
employees about cyber
and preventive measure

6. Enforce Policies

Impose strict security po
such as the frequency o
and strength of passwor

7. Respond and Recov

Ensure cyber incident re
and recovery plans are r
and can be effectively
implemented

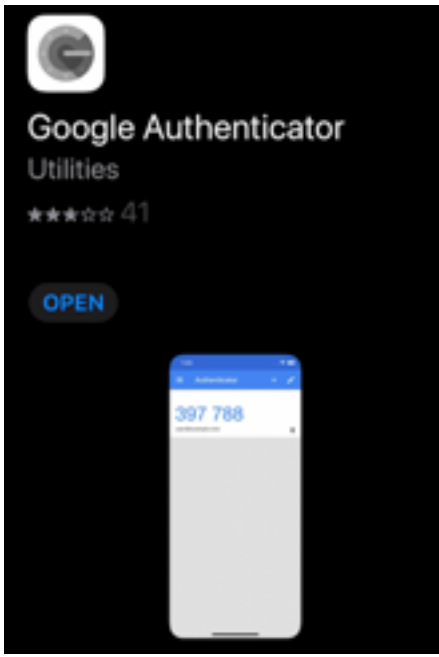
Want to learn more?
Visit www.csa.gov.sg

Source : www.csa.g

eves

What you can do to protect yourself

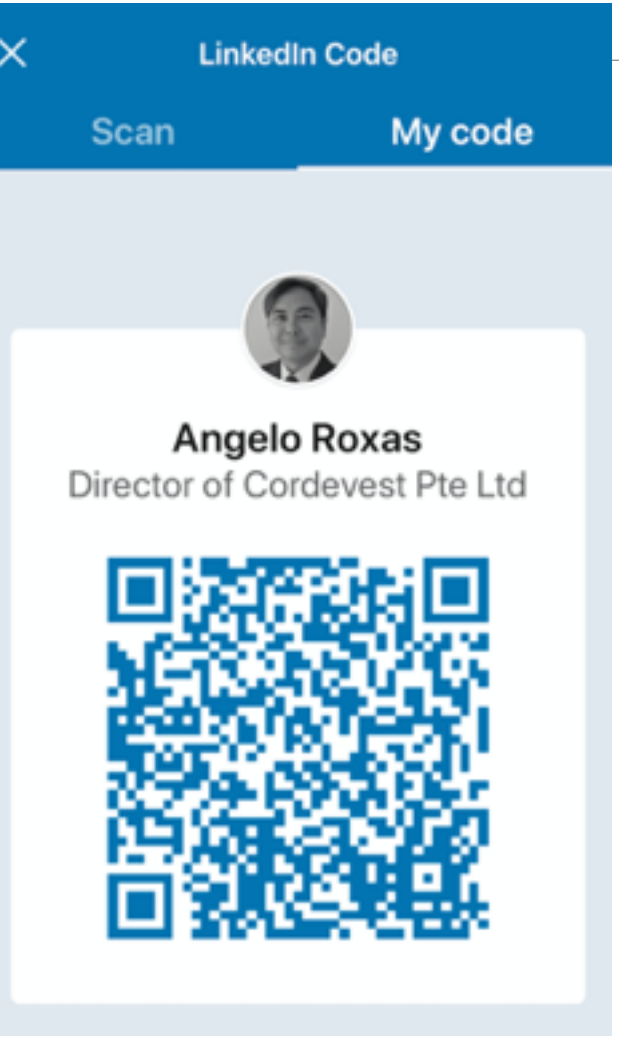
- Employ proper cyber hygiene
- Update home WiFi with a strong password
- Never click on ***COVID-19*** related attachments
- Right click emails to ensure the links are the correct domain
- Use 2 FA to access personal emails, etc



WANNACRY Case study

WANNACRY – THE RANSOMWARE EVENT OF 2017 SO FAR

- The sweeping WannaCry ransomware event that commenced on 12 May 2017 has been revealed to use two separate previously leaked Equation Group tools, and the current strain—but by **no means the final strain**—has been **effectively killed** due to a researcher registering a hardcoded domain in the ransomware
- It propagated through **EternalBlue, an exploit for older Windows systems the DoublePulsar tool to install and execute a copies of itself**. EternalBlue was stolen and leaked by a group called **The Shadow Brokers** a few months prior to the attack.
- The WannaCry ransomware epidemic appears to have ended as abruptly as it started, although not without first having infected +**230,000 endpoints** in **more than 150 countries**, many of them in the medical and manufacturing industries
- The WannaCry outbreak also made extensive use of Equation Group tools, yet no one is suggesting that the Equation group is responsible for WannaCry, at least not directly.
- **Careful planning** appears to have gone into this event, including releasing the ransomware on a Friday, perhaps to increase chaos and response time for victims — a **familiar tactic from other high-profile criminal attacks**, such as the Bangladesh Bank crime. That the WannaCry variant was in more than **24 languages** also suggests lofty goals for the criminals
- The 97 transactions to the three hardcoded bitcoin addresses totaling approximately USD 25,000-, a very **modest amount** Based on our research regarding ransomware payments, we've seen even a small-time operation earning approximately USD 100,000 over a few months



Useful links :

https://thecybersecurityplace.com/cybersecurity-and-covid-19-the-first-100-days

https://www.mimecast.com/globalassets/cyberesilience-content/100-days-of-coronavirus-threat-intelligence.pdf

Angelo.Roxas@Cordevest.com
+65 9234 9948

Q & C?