Security of Work From Home

Yu On Ng | Security Consultant | May 2020

Today Agenda

1. Secure remote access
   a) Common remote access technologies
   b) Recommendations

2. Secure video conference
   a) Latest security incidents
   b) Major security threats
   c) Our advices

3. Other security tips

About Us

Hong Kong Computer Emergency Response Team Coordination Centre (香港電腦保安事故協調中心)

Mission:
As the **Centre for coordination** of computer security incident response for local enterprises and Internet Users, and the **International Point-of-Contact**

- Founded in 2001
- Funded by Government
- Operated by Hong Kong Productivity Council

Website: www.hkcert.org
24-hour Hotline: 8105 6060
Email: hkcert@hkcert.org

HKCERT services

01 Security Alert Monitoring and Early Warning

02 Report and Response

03 Publication of Security Guidelines and Informatior

04 Promotion of Information Security Awareness

Secure
Remote Access

Common Technologies

Remote Desktop Control

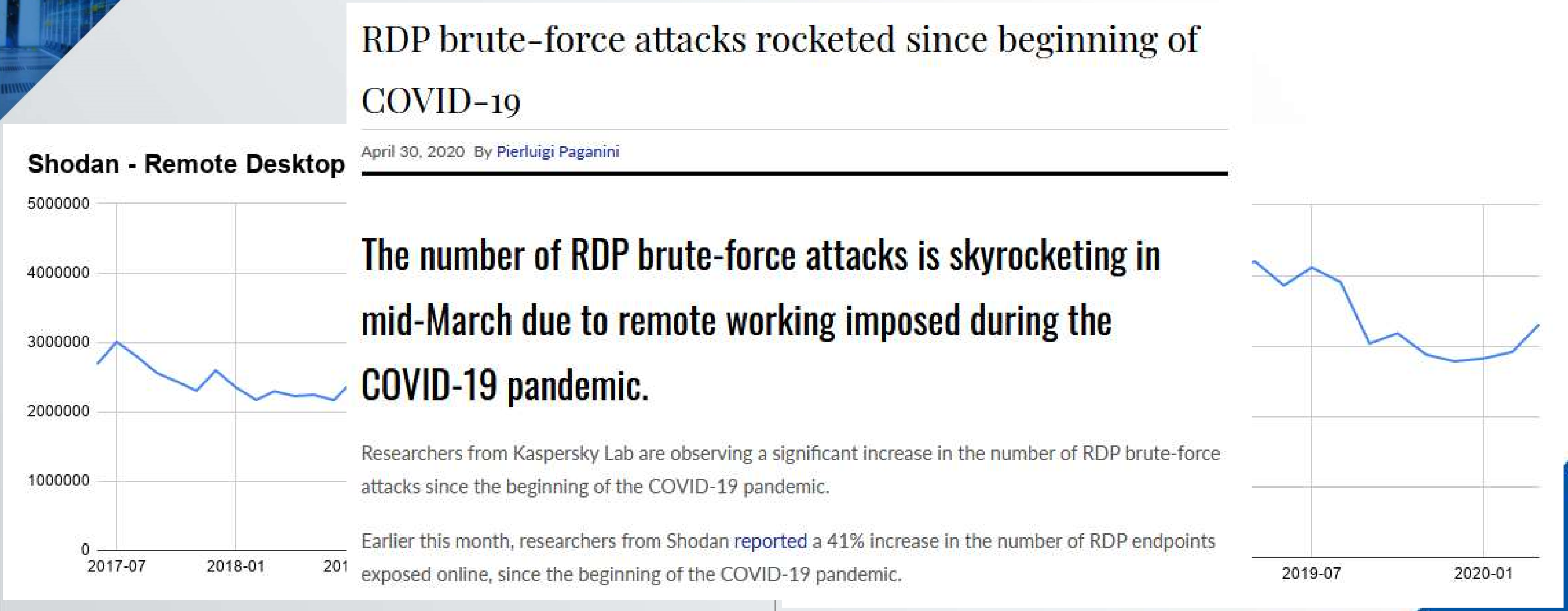
Virtual Private Network

Virtual Desktop infrastructure

Major security risks

- Unpatched software vulnerability
- Improper setting of data encryption or poor encryption key management
- Easy guess password
- Connect via untrusted network
- Weak end point security, e.g. outdated anti-virus
- Loss or theft

Increase in exposure During COVID-19 and also Cyber Attack



RDP brute-force attacks rocketed since beginning of COVID-19

April 30, 2020 By Pierluigi Paganini

The number of RDP brute-force attacks is skyrocketing in mid-March due to remote working imposed during the COVID-19 pandemic.

Researchers from Kaspersky Lab are observing a significant increase in the number of RDP brute-force attacks since the beginning of the COVID-19 pandemic.

Earlier this month, researchers from Shodan reported a 41% increase in the number of RDP endpoints exposed online, since the beginning of the COVID-19 pandemic.

https://securityaffairs.co/wordpress/102495/hacking/covid-19rdp-bruteforce-attacks.html

Recommendations

DON'T Rush to Set Up Infrastructure.
DO Adopt Secure Design Principles

For Organisation

Provide remote access security policy

- Ensure all staff fully understand the rules of using the relevant services

Review the security configuration regularly, e.g. encryption,

- Ensure the software is updated and security configurations are tightened
- Details can refer to HKCERT “Best Practice Guide of Remote Desktop (for corporate administrator)”

Review user list and the access right regularly

- Ensure each employee can only access the systems resources required for their work

Set up log monitoring and alert mechanism

- Any abnormal logs or suspicious traffic should trigger alert and notify relevant staff immediately. Incident investigation should be conducted.

Enable 2-Factor Authentication /Multi-factors authentication

- For all privileged and non-privileged accounts

■Consider DDoS protection solution

- Protect against DDoS to ensure systems availability

For Users

Install anti-virus and set up auto-update

- Only connect to the company network from a secured device and network environment

Always update the remote access software to latest version, if any

- Set up auto-update for the software and Windows

Enable the 2FA / MFA feature

- And use a strong password

Beware of phishing and social engineering attacks

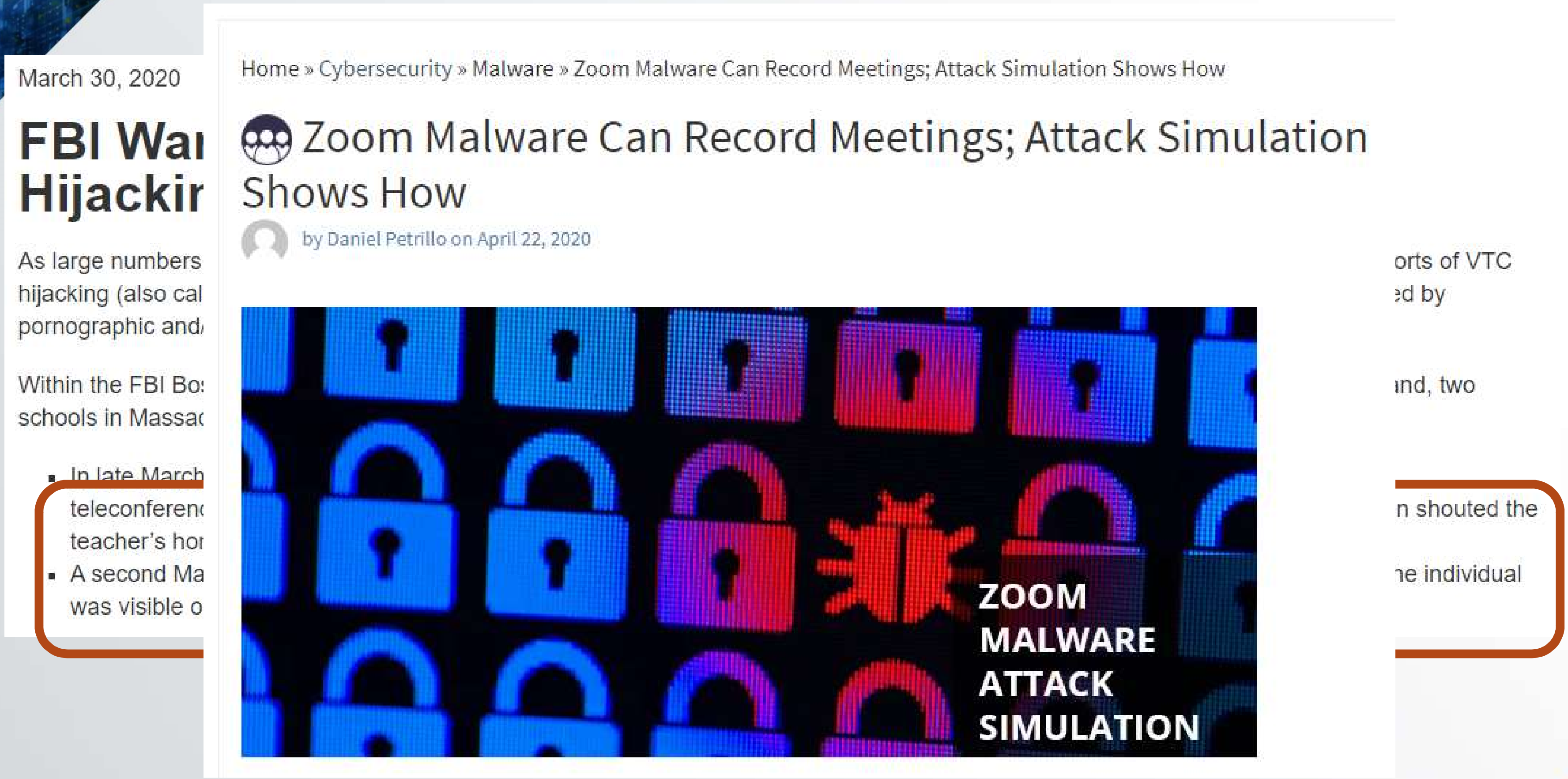
- DO NOT provide sensitive information to unknown person or website

- **Keep your remote access devices securely**

  - Report to your company immediately for any loss and theft

Secure Video Conference

Security incidents Worldwide



March 30, 2020

FBI Wa

Hijackir

As large numbers … orts of VTC
hijacking (also cal … ed by
pornographic and/

Within the FBI Bos … and, two
schools in Massac

- In late March
teleconferenc … n shouted the
teacher's hor
- A second Ma … e individual
was visible o

Home » Cybersecurity » Malware » Zoom Malware Can Record Meetings; Attack Simulation Shows How

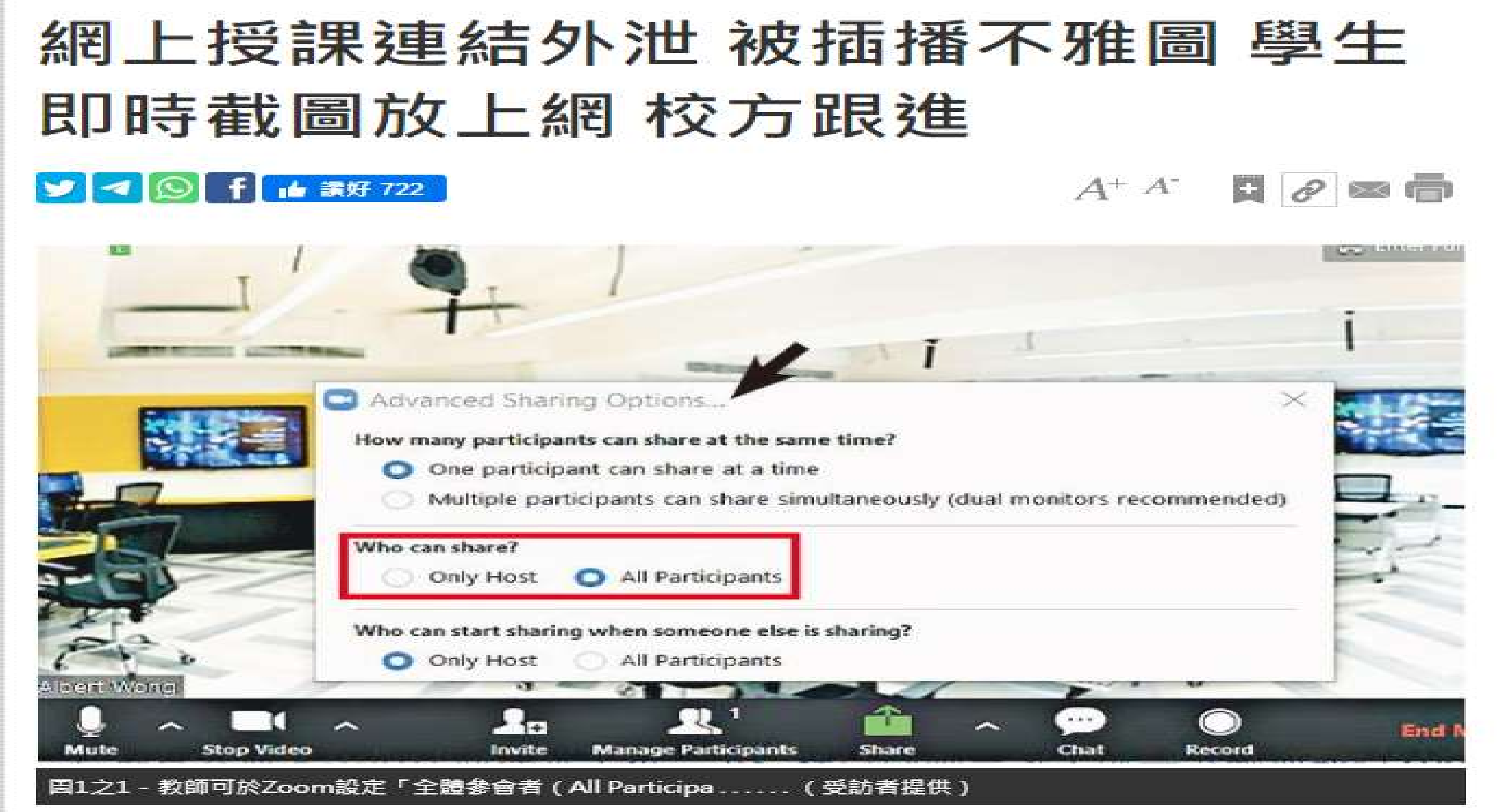
Zoom Malware Can Record Meetings; Attack Simulation Shows How

by Daniel Petrillo on April 22, 2020

https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

https://securityboulevard.com/2020/04/zoom-malware-can-record-meetings-attack-simulation-shows-how/

Rising concerns in HK as it happened in HK too…



網上授課連結外泄 被插播不雅圖 學生即時截圖放上網 校方跟進

How many participants can share at the same time?

● One participant can share at a time
○ Multiple participants can share simultaneously (dual monitors recommended)

Who can share?

○ Only Host ● All Participants

Who can start sharing when someone else is sharing?

● Only Host ○ All Participants

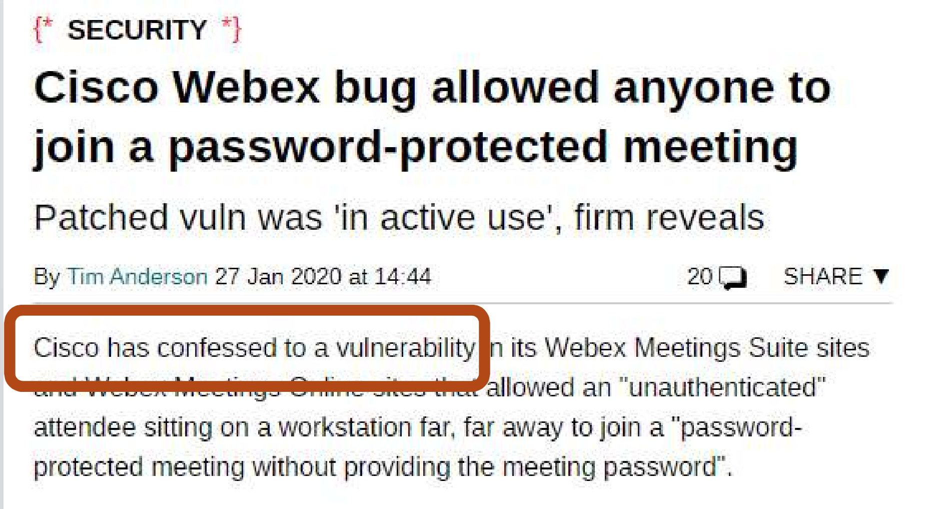
圖1之1 - 教師可於Zoom設定「全體參會者（All Participa ...... （受訪者提供）

https://news.mingpao.com/ins/要聞/article/20200311/s00001/1583865891033/網上授課連結外泄-被插播不雅圖-學生即時截圖放上網-校方跟進

https://www.scmp.com/news/hong-kong/education/article/3075287/hong-kong-government-and-schools-talks-over-zoom-security

Zoom is not the only one has security issues

System vulnerability



{* SECURITY *}

Cisco Webex bug allowed anyone to join a password-protected meeting

Patched vuln was 'in active use', firm reveals

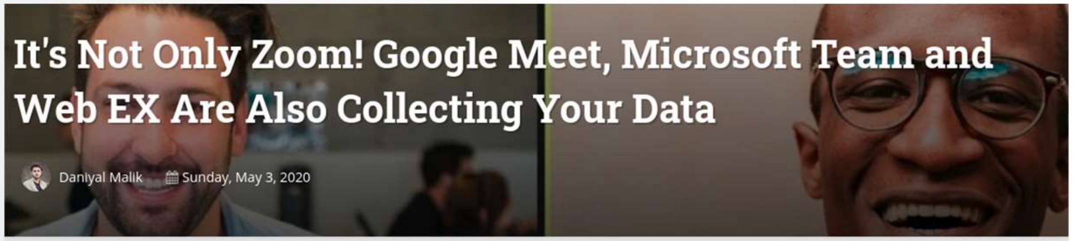
By Tim Anderson 27 Jan 2020 at 14:44 20 SHARE ▼

Cisco has confessed to a vulnerability in its Webex Meetings Suite sites and Webex Meetings Online sites that allowed an "unauthenticated" attendee sitting on a workstation far, far away to join a "password-protected meeting without providing the meeting password".

https://www.digitalinformationworld.com/2020/05/it-s-not-only-zoom-google-meet-microsoft-team-and-web-ex-are-also-collecting-your-data.html

Privacy issue

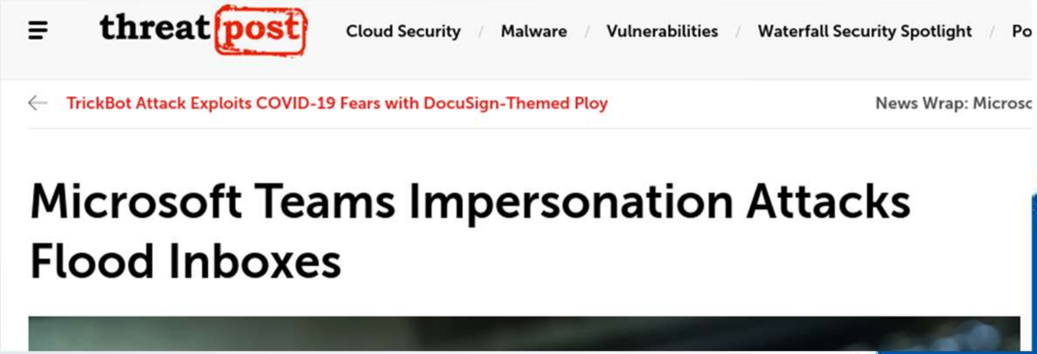
https://www.digitalinformationworld.com/2020/05/it-s-not-only-zoom-google-meet-microsoft-team-and-web-ex-are-also-collecting-your-data.html



It's Not Only Zoom! Google Meet, Microsoft Team and Web EX Are Also Collecting Your Data

Daniyal Malik Sunday, May 3, 2020

Cyber attack



TrickBot Attack Exploits COVID-19 Fears with DocuSign-Themed Ploy

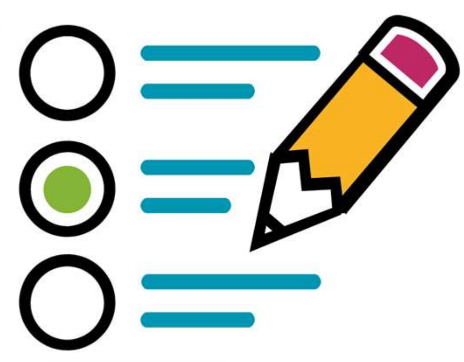
News Wrap: Microsc

Microsoft Teams Impersonation Attacks Flood Inboxes

https://threatpost.com/microsoft-teams-impersonation-attacks/155404/

In terms of security, how to choose the VC software?

- **Conduct risk assessment**
  - Data classification, e.g. has confidential information ?
  - Understand the threats and root causes. In general 2 types
    - Vulnerability
    - Mis-configuration



- **Mitigate the risks**
  - Choose the one with good track record in patching security loopholes, and regular update
  - Set up security controls, e.g. administrative, preventive and corrective

- **Perform testing**
  - Ensure the controls work as expected

3 Major Security Threats

Image credit: **https://economictimes.indiatimes.com/tech/internet/69-indian-firms-face-serious-cyber-attack-risk-study/articleshow/69305216.cms**

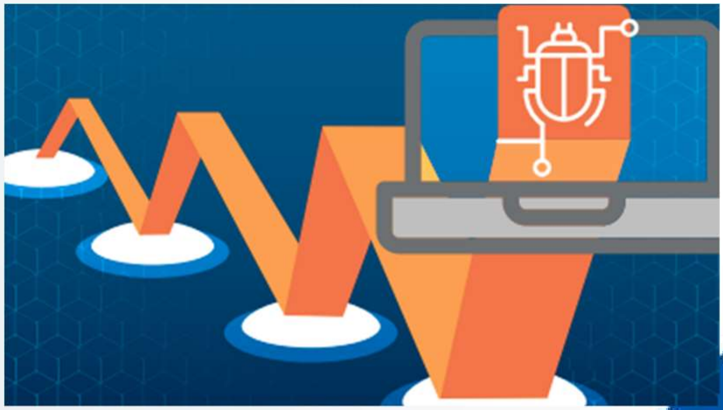
#1 Unauthorised access (e.g. hijacking)

- Unauthorised people entered the class or meeting (e.g. zoombombing)
  - By guessing the meeting link and ID and go into the meeting to do so
- Impact
  - Show inappropriate content such as violent images and pornography
  - Harassment
  - Confidentiality

#2 Spread Malware / Suspicious URL

- Use chat room function to send malware or phishing URL
  - Previous UNC vulnerability of Zoom allow stealing of Windows logins

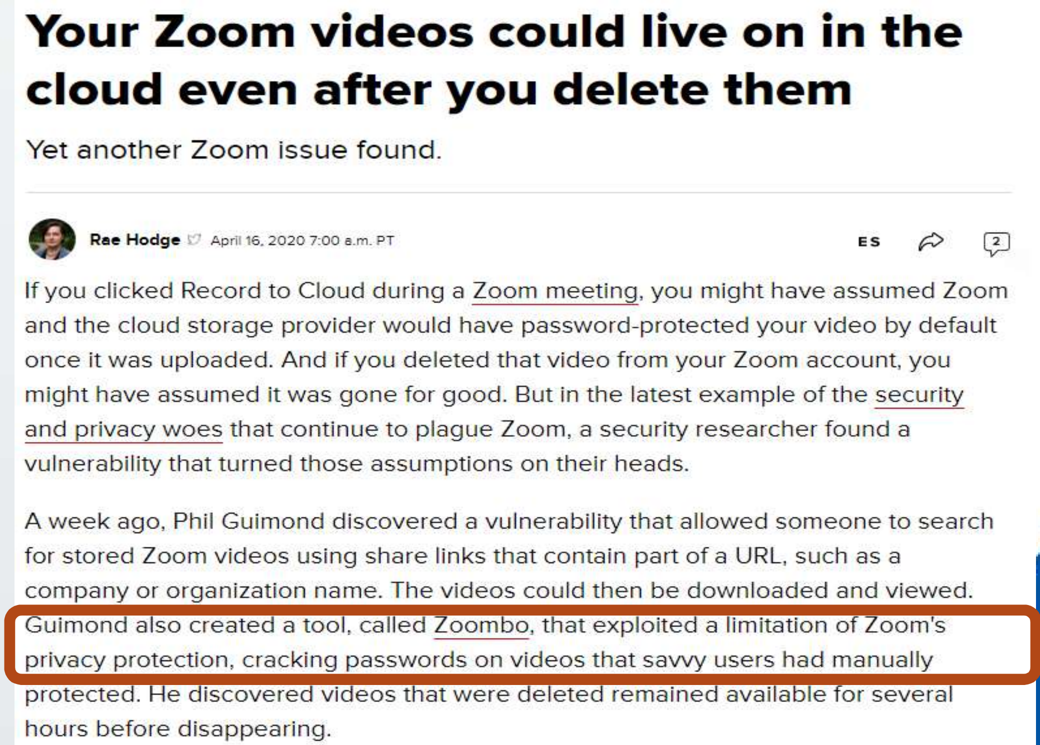
- Impact
  - Ransomware
  - Steal confidential information
  - Money fraud



#3 Privacy issues

- Recording saved in cloud could be viewed by unauthorised party

- Impact
  - Information leakage
  - Lawsuit
  - Affect reputation and trust



Your Zoom videos could live on in the cloud even after you delete them

Yet another Zoom issue found.

Rae Hodge April 16, 2020 7:00 a.m. PT

If you clicked Record to Cloud during a Zoom meeting, you might have assumed Zoom and the cloud storage provider would have password-protected your video by default once it was uploaded. And if you deleted that video from your Zoom account, you might have assumed it was gone for good. But in the latest example of the security and privacy woes that continue to plague Zoom, a security researcher found a vulnerability that turned those assumptions on their heads.

A week ago, Phil Guimond discovered a vulnerability that allowed someone to search for stored Zoom videos using share links that contain part of a URL, such as a company or organization name. The videos could then be downloaded and viewed. Guimond also created a tool, called Zoombo, that exploited a limitation of Zoom's privacy protection, cracking passwords on videos that savvy users had manually protected. He discovered videos that were deleted remained available for several hours before disappearing.

https://www.cnet.com/news/your-zoom-videos-could-live-on-in-the-cloud-even-after-you-delete-them/

Security Advices

Image credit: **https://www.century-it.co.uk/cyber-security-advice-and-help/**

Preparation

- Set up security and acceptable user policy
- Keep the VC software is up-to-date
- Make classroom private and deny trespassers
- Do not disclose meeting link and password. Send to authorised user (e.g. student) separately
- Use different meeting ID & passwords for different class
- Enable waiting room function

Meeting in progress

- Limit what participant can do. Allow only when necessary, e.g. video, audio, screen sharing, chat
- Monitor the class for inappropriate content
- Give participants a prior notice if you will record
- Save the recording to PC instead of cloud
- Lock the meeting once everyone has joined

When Prevention Fails: Incident Response Preparedness

When conducting the class / meeting

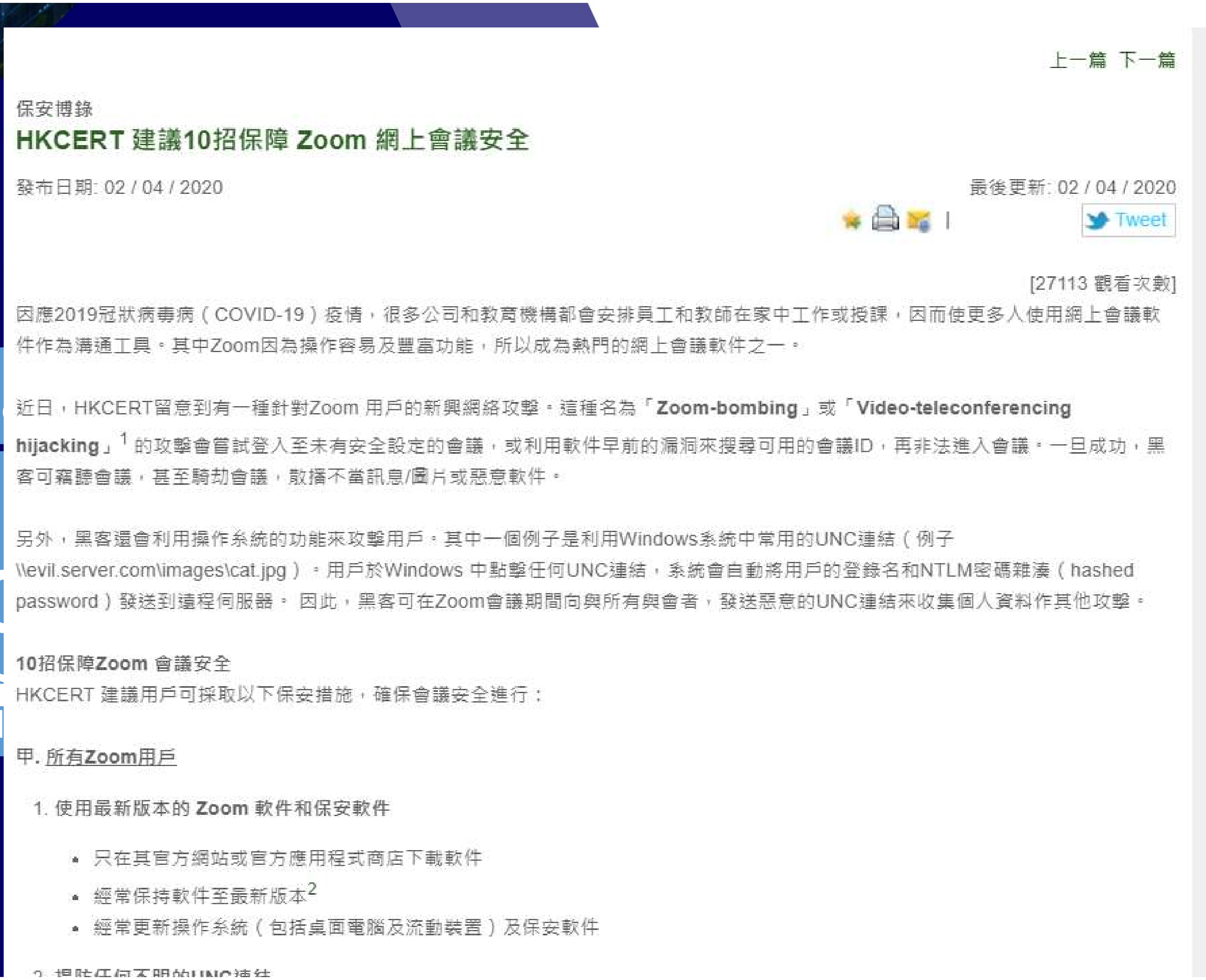
- Remove malicious content and participants immediately

After the class / meeting

- Change related meeting ID and password
- Update your OS, VC software and anti-virus software
- Perform full system scan

HKCERT

10 Me
Zoom
建議10
網上會



上一篇 下一篇

保安博錄

HKCERT 建議10招保障 Zoom 網上會議安全

發布日期: 02 / 04 / 2020

最後更新: 02 / 04 / 2020

[27113 觀看次數]

因應2019冠狀病毒病（COVID-19）疫情，很多公司和教育機構都會安排員工和教師在家中工作或授課，因而使更多人使用網上會議軟件作為溝通工具。其中Zoom因為操作容易及豐富功能，所以成為熱門的網上會議軟件之一。

近日，HKCERT留意到有一種針對Zoom 用戶的新興網絡攻擊。這種名為「**Zoom-bombing**」或「**Video-teleconferencing hijacking**」[1] 的攻擊會嘗試登入至未有安全設定的會議，或利用軟件早前的漏洞來搜尋可用的會議ID，再非法進入會議。一旦成功，黑客可竊聽會議，甚至騎劫會議，散播不當訊息/圖片或惡意軟件。

另外，黑客還會利用操作系統的功能來攻擊用戶。其中一個例子是利用Windows系統中常用的UNC連結（例子 \\evil.server.com\images\cat.jpg）。用戶於Windows 中點擊任何UNC連結，系統會自動將用戶的登錄名和NTLM密碼雜湊（hashed password）發送到遠程伺服器。 因此，黑客可在Zoom會議期間向與所有與會者，發送惡意的UNC連結來收集個人資料作其他攻擊。

10招保障Zoom 會議安全

HKCERT 建議用戶可採取以下保安措施，確保會議安全進行：

甲. 所有Zoom用戶

1. 使用最新版本的 **Zoom** 軟件和保安軟件

- 只在其官方網站或官方應用程式商店下載軟件
- 經常保持軟件至最新版本[2]
- 經常更新操作系統（包括桌面電腦及流動裝置）及保安軟件

2. 提防任何不明的UNC連結

Security tips

Bring these messages back to your organization…

1. Never Share the **Work Device's Account** with Others
2. Ensure **Privacy** in the Working Environment
3. Ensure **Security** of Working Environment
4. Ensure **Wi-Fi Connection** is Secured
5. Encrypt and backup the **Data**
6. Strictly Comply with **Company Information Security Policies**

Contact your

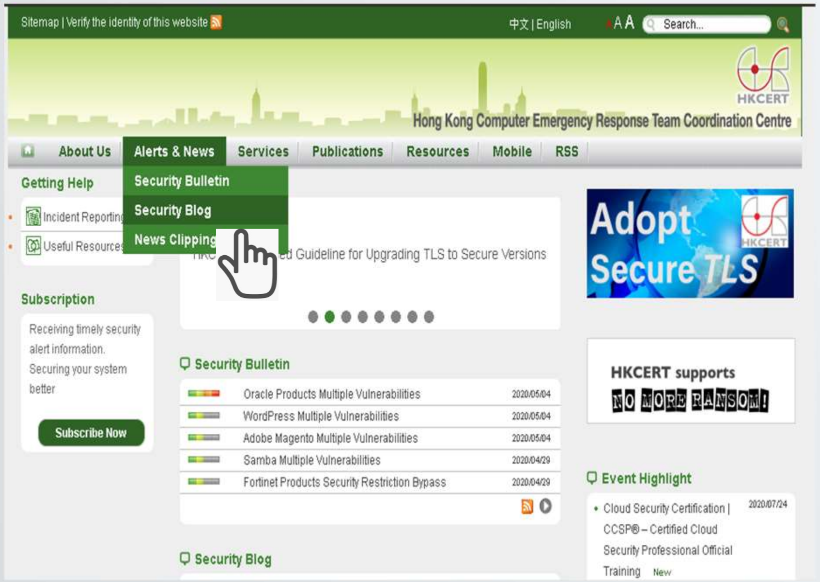
IT Department immediately! if you

have one…

Report to police if any **financial loss** is occurred

More useful security articles

HKCERT Blogs



HKC… …ed Guideline for Upgrading TLS to Secure Versions

Subscription

Receiving timely security alert information.
Securing your system better

Security Bulletin

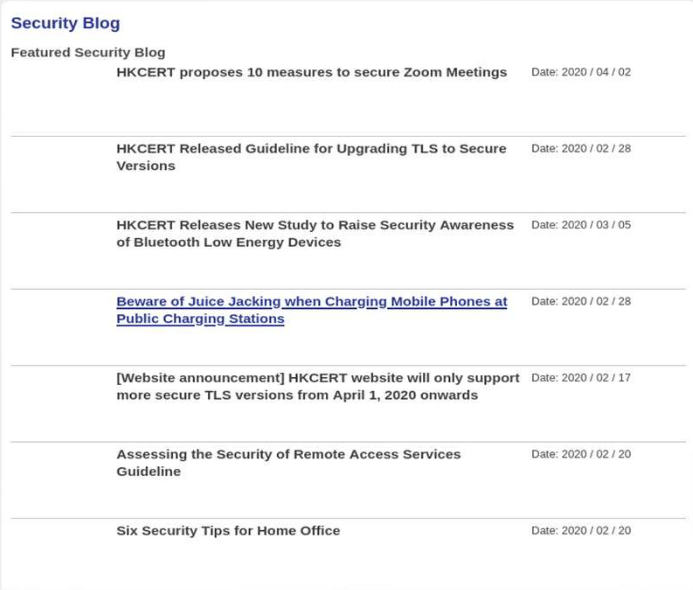
Oracle Products Multiple Vulnerabilities	2020/05/04
WordPress Multiple Vulnerabilities	2020/05/04
Adobe Magento Multiple Vulnerabilities	2020/05/04
Samba Multiple Vulnerabilities	2020/04/29
Fortinet Products Security Restriction Bypass	2020/04/29

HKCERT supports NO MORE RANSOM!

Event Highlight

- Cloud Security Certification | CCSP® – Certified Cloud Security Professional Official Training New 2020/07/24

Security Blog



Security Blog

Featured Security Blog

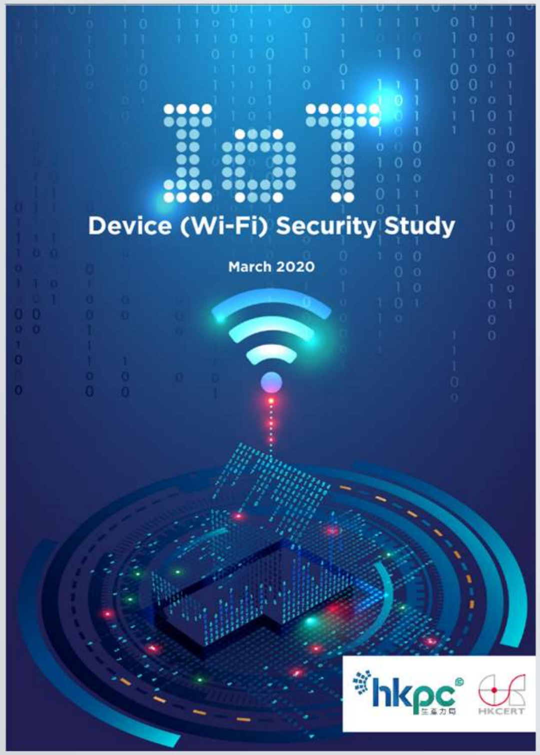
HKCERT proposes 10 measures to secure Zoom Meetings	Date: 2020 / 04 / 02
HKCERT Released Guideline for Upgrading TLS to Secure Versions	Date: 2020 / 02 / 28
HKCERT Releases New Study to Raise Security Awareness of Bluetooth Low Energy Devices	Date: 2020 / 03 / 05
Beware of Juice Jacking when Charging Mobile Phones at Public Charging Stations	Date: 2020 / 02 / 28
[Website announcement] HKCERT website will only support more secure TLS versions from April 1, 2020 onwards	Date: 2020 / 02 / 17
Assessing the Security of Remote Access Services Guideline	Date: 2020 / 02 / 20
Six Security Tips for Home Office	Date: 2020 / 02 / 20

1. Go to https://www.hkcert.org
2. Select "Alerts & News" -> "Security Blog"

1. Find the blog by title, or filter by date

Security Guidelines and Reports

IoT Guidelines

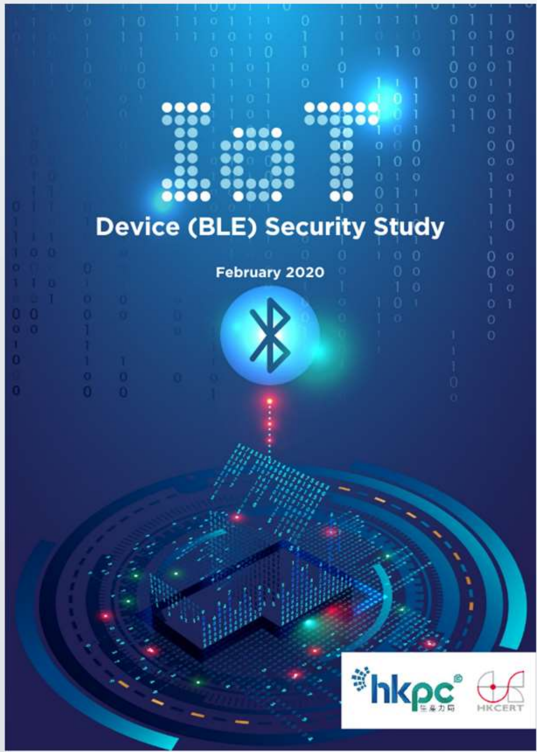


IoT

Device (Wi-Fi) Security Study

March 2020

hkpc HKCERT



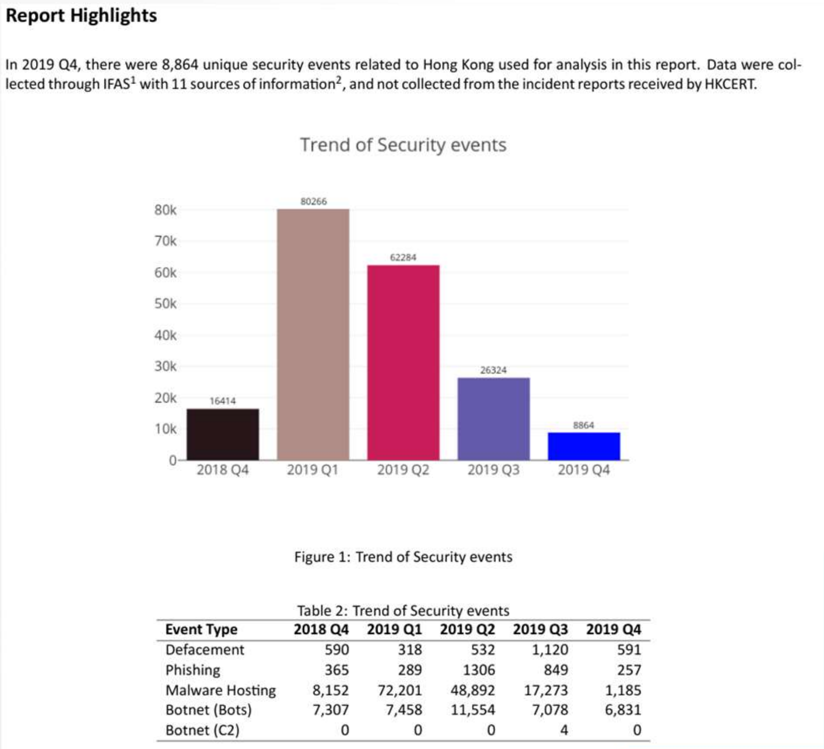
IoT

Device (BLE) Security Study

February 2020

hkpc HKCERT

Security Watch Report



Report Highlights

In 2019 Q4, there were 8,864 unique security events related to Hong Kong used for analysis in this report. Data were collected through IFAS[1] with 11 sources of information[2], and not collected from the incident reports received by HKCERT.

Figure 1: Trend of Security events

Table 2: Trend of Security events

Event Type	2018 Q4	2019 Q1	2019 Q2	2019 Q3	2019 Q4
Defacement	590	318	532	1,120	591
Phishing	365	289	1306	849	257
Malware Hosting	8,152	72,201	48,892	17,273	1,185
Botnet (Bots)	7,307	7,458	11,554	7,078	6,831
Botnet (C2)	0	0	0	4	0

Thank You

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 6168   www.hkpc.org