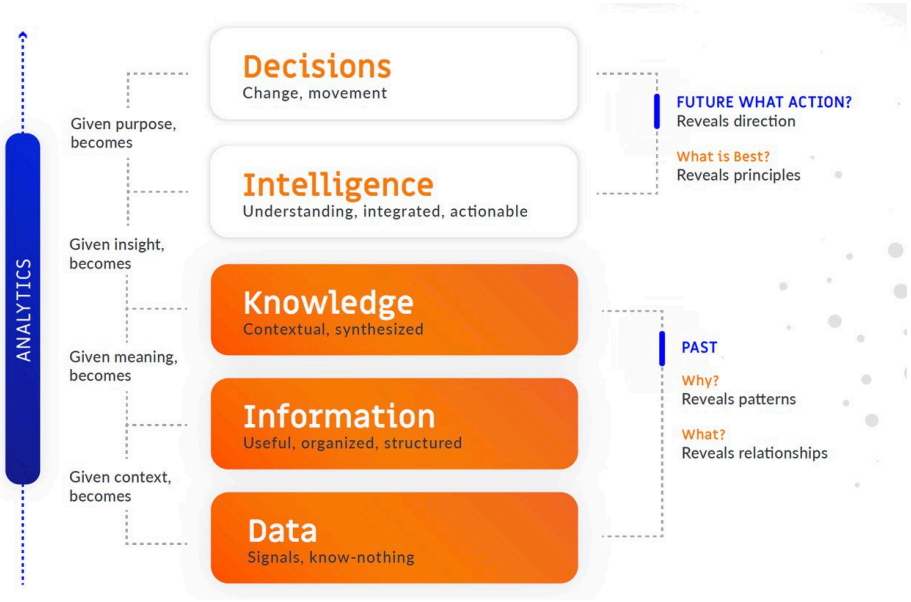
Weekly Intelligence Summary

Apr 10, 2020 (Pandemic)

In the spotlight this week: The vulnerabilities found in Zoom definitely should be a BIG topic to all people in #HongKong especially during this pandemic era. There are a few points of concerns: (1) Privacy issue, (2) UNC path injection, (3) 2 0days on Mac, (4) end-to-end encryption was defined as endpoint to server only. I personal think that #Zoom is not malware. #Zoom is a good service but like most of the technology security is not put in design. I shall use #Zoom as normal business and casual online meeting. (cisp-id:7318) Another interesting vulnerability was coming from a blog post by 360.cn. The alarming DarkHotel (APT-C-06) was found attacking Chinese Institutions via exploiting the SangFor VPN. Not sure the attribution, but it also links to the same pandemic event. (cisp-id:7261)

TL;DR

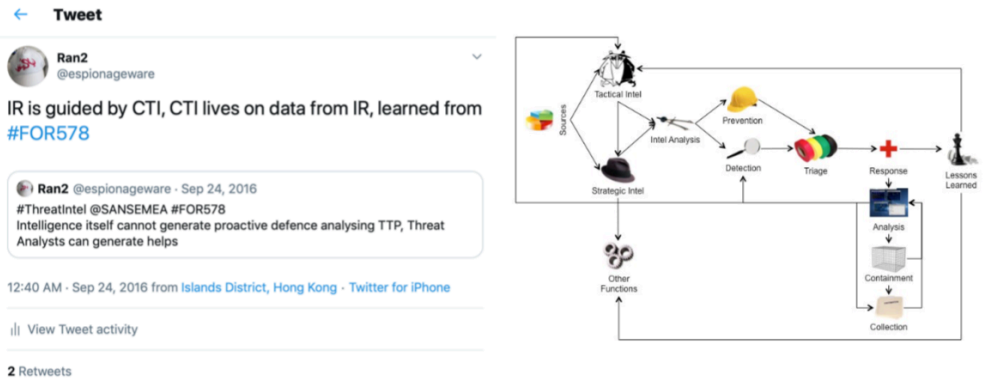
This is the first Weekly Intelligence Summary issued in 2020. In the past years, I tried to provide the latest cyber threat intelligence updates to some of my clients especially friends who are working in cybersecurity of the financial industries in Hong Kong. The term Cyber Threat Intelligence means different to different people. Some told me it is useless, some told me only IOCs are useful because they can import them into their SIEM solution, some told me it is a must part for building their SOC. I have no answer for you but can only provide you a screen shot captured from unknown source that my buddy sent me today. (Fig. 1)



(Fig. 1 – from Vincent)

Starting from this week, I decided to put all my casual views (pleases forgive my low-level language skill) on the latest cybersecurity threat news in a 2-pages writing instead of posting my comments on a Whatsapp group. I also decided to rebuild our MISP instance collections with a new dashboard which will be able to offer for subscription by next month – I hope the pandemic period will be put an end next month, under my optimistic assumption.

Some of you may aware I have re-modelled DATC as DFIR consultancy firm to provide services in BEC, compromise assessment and VAPT. I am a strong believer of the statement of: IR is guided by CTI, CTI lives on data from IR. (Fig. 2) This may be this is the main reason why I start to write this weekly intelligence summary.



(Fig. 2 – IR life cycle starts from threat intel)

(cisp-id:7318) March 30, 2020
FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.
https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

(cisp-id:7318) April 3, 2020
Zoom's privacy and security woes in the spotlight. The seemingly insatiable demand among people and businesses alike helps reveal a rash of privacy and security issues facing the platform, Welivesecurity posted. The app's maker is weathering a storm of criticism from various quarters, including privacy advocates, security experts, several U.S. state attorneys general, a U.S. lawmaker, and the FBI. Bad news have kept piling up in recent days, prompting the company to respond.
https://www.welivesecurity.com/2020/04/03/zoom-privacy-security-spotlight/

(cisp-id:7261) April 6, 2020
Recently, Qihoo 360 detected an APT attack that deliver malicious files through hijacked security services of a domestic VPN provider. We have reported the vulnerability details to the service provider and received confirmation. Further reversing shows that the attack can be attributed to the Darkhotel (APT-C-06), an APT gang in the Korean Peninsula. Since March this year, more than 200 VPN servers have been compromised and many Chinese institutions abroad were under attack. In early April, the attack spread to government agencies in Beijing and Shanghai.

The monitoring and analysis also suggest that a large number of VPN servers and endpoint devices in associated functioning units have been under the control of the attackers.
~~https://blogs.360.cn/post/APT_Darkhotel_attacks_during_coronavirus_pandemic.html~~
Google Cache: https://bit.ly/34vsrwG (the blog post is not available for access today)

DATC comments (updated on Apr 12, 2020)

Threat Intelligence ▾ | CVE ▾ | Lookalike Domains ▾ | Bitcoin Abuse Search ▾ | Search ▾ | App Cyber Threat Intelligence

DATC Comments

Time Range

Last 30 days | Submit | Hide Filters

date	event_id	category	type	ioc
2020-04-06	7261	Other	comment	Interesting ... Qihoo 360 seems take down this blog today (Apr 12, 2020). The blog did not provide much solid evidence to attribute the DarkHotel group and also mentioned SangforUD.exe VPN client embedded APT from East Asia attacking BJ and Shanghai to monitor transportation routes of pandemic materials. I can't see the agencies names but seems related to 北京各区工会 and 上海街道居委. My concern on the vulnerabilities (seems 0-days) on Sangfor VPN that some financial organizations in Hong Kong may installed for their branches in China. If that is the case, they need to patch their Sangfor systems and consider to apply
2020-04-03	7318	Other	comment	#Zoom is not malware. #Zoom is a good service but like most of the technology security is not put in design. I shall use #Zoom as normal business and casual online meeting. I personally think that the vulnerabilities are easily be found in all applications, including Facebook, Telegram, WhatsApp and WeChat. Zoom should not be banded. For the regulators or government departments, they have their reasons to band Zoom, but during this Pandemic period, we need to find out a replacement for the communities before we can just say do use it. Here is some pains for me to use other tools: I spent 10-mins to configure Skype Business for an online meeting I need to register an Microsoft Account to use Microsoft Team I need to Install again my Cisco Webex Meeting client an online session I just download and testing WickrPro I think we can condemn Zoom for the missing security features in the past, but I have to face a reality to teach my wife (for an example, only) to use other new video communication tools for FREE with her friends during the pandemic period.):