YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

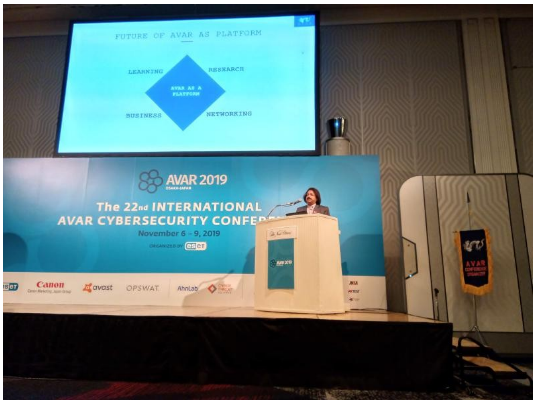
November 2019

Contents

AVAR 2019

<web-link for this article>

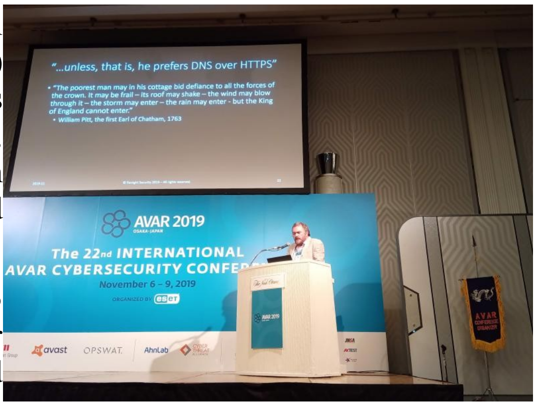
Righard Zwienenberg opens the 22nd AVAR conference, the 4th to be held in Japan



AVAR CEO Kesavardhanan Jayaraman presents AVAR as a Platform.

The 22nd international AVAR Cybersecurity Conference was held in Osaka, Japan on 6 - 9 November 2019. Conference organiser Righard Zwienenberg reported that there was a record number of submissions on the Call for Papers, and the 9 referees considered they were, "extremely good quality", prompting a change to a two-track conference, to accommodate more speakers. CEO Kesavardhanan Jayaraman explained the latest developments in AVAR, and his vision for AVAR as a platform to reach beyond anti-malware experts to bring a security message to a larger audience.

In the keynote speech, Internet pioneer Dr. Paul Vixie advocated against DNS over HTTPS (DoH) as it shifted control further away from the user. This gives a false sense of security, unless a VPN is used, browsing behaviour can still be inferred from connections made, and breaks parental control and corporate network control.


"...unless, that is, he prefers DNS over HTTPS"

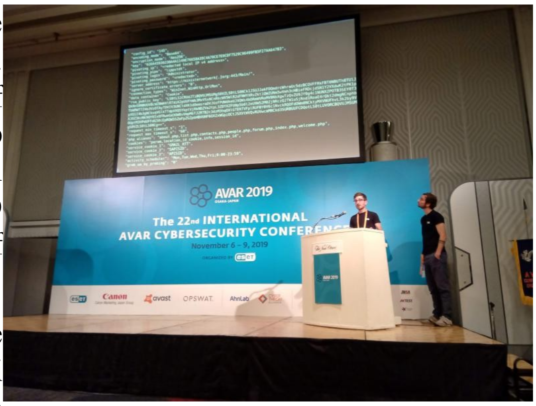
- "The poorest man may in his cottage bid defiance to all the forces of the crown. It may be frail – its roof may shake – the wind may blow through it – the storm may enter – the rain may enter - but the King of England cannot enter."
  - William Pitt, the first Earl of Chatham, 1763

Paul Vixie updates William Pitt's 1763 quote.

Other papers covered a wide range of topics. It is no longer a surprise that money is a strong motive for malware developers. Yoshihiro Ishikawa explained how the HYDSEVEN APT steals cryptocurrency. These papers examine some of the many ways that criminals are attacking financial systems. Augusto Remillano and Hazel Poligratis reported on the Rocke group hijacking Linux servers to mine cryptocurrency. Dinesh Devadoss and

Kaarthik R Muthukrishnan looked at how Macs are exploited to steal from cryptocurrency exchanges. Heungsoo Kang examined APT attacks of employees at cryptocurreny exchanges. Josep Albors looked at attacks on users of traditional online banking in Japan. Rommel Abraham D Joven's paper covered online digital skimming of credit cards.

Mobile and IoT topics were covered. GenShen Ye described advanced IoT malware. Dhanalakshmi Velusamy described targetted Android attacks in Japan and Hsun-Jen Hsu, Jen-Yu Tsai gave a tutorial on the Android tool Frida.



Matthieu Faou and Thomas Dupuy cover a tricky point on Operation Ghost.

Author and well-known expert in security and malwar, Eddy Willems was excited to chair the Day 1 session.

Many papers studied particular APT threats, including Ghost, HYDSEVEN, 8.t, APT10, SWEETCANDLE, SOURCANDLE, and POISONPLUG.

However, a worrying trend is the rise of Cyber Espionage. There are definite indications that nation-states are extending their traditional spying activities into the cyber-domain. Operation Ghost, Tick Tock and ATTOR are all threats with espionage features, and Buhtrap has shifted from a focus on crime to espionage, as documented by Anton Cherepanov and Jean-Ian Boutin.

SINGLE COUNTRY, MULTIPLE PRODUCTS
AVAR 2019
The 22nd INTERNATIONAL
AVAR CYBERSECURITY CONFERENCE

Best Speaker Mark Lechtik on North Korea's Anti-Virus software.

The conference delegates voted Mark Lechtik the Best Speaker, for his paper on North Korea's Anti-Virus programs.

The conference also featured a Gala Dinner, with drumming, magic and ninjas.

AVAR (Association of anti Virus Asia Researchers) was formed in June, 1998 with a mission to prevent the spread of malware and the damage caused by it. AVAR aims to do this by developing cooperative relationships among anti-malware experts in Asia. AVAR is an independent and non-profit organization which focuses on the Asia Pacific region and consists of prominent experts from 18 territories including China, India, Japan, USA, Vietnam, Hong Kong, South Korea, Philippines, Germany, and Slovakia.

GenShen Ye on IoT malware in track 2.

AVAR 2019
"ROCKE"
Specializes in cryptomining
Quick incorporation of exploits for vulnerabilities of software applications
Actively engages in distributing and executing cryptomining malware using a varied toolkit
AVAR 2019
The 22nd INTERNATIONAL
AVAR CYBERSECURITY CONFERENCE
November 6 – 9, 2019

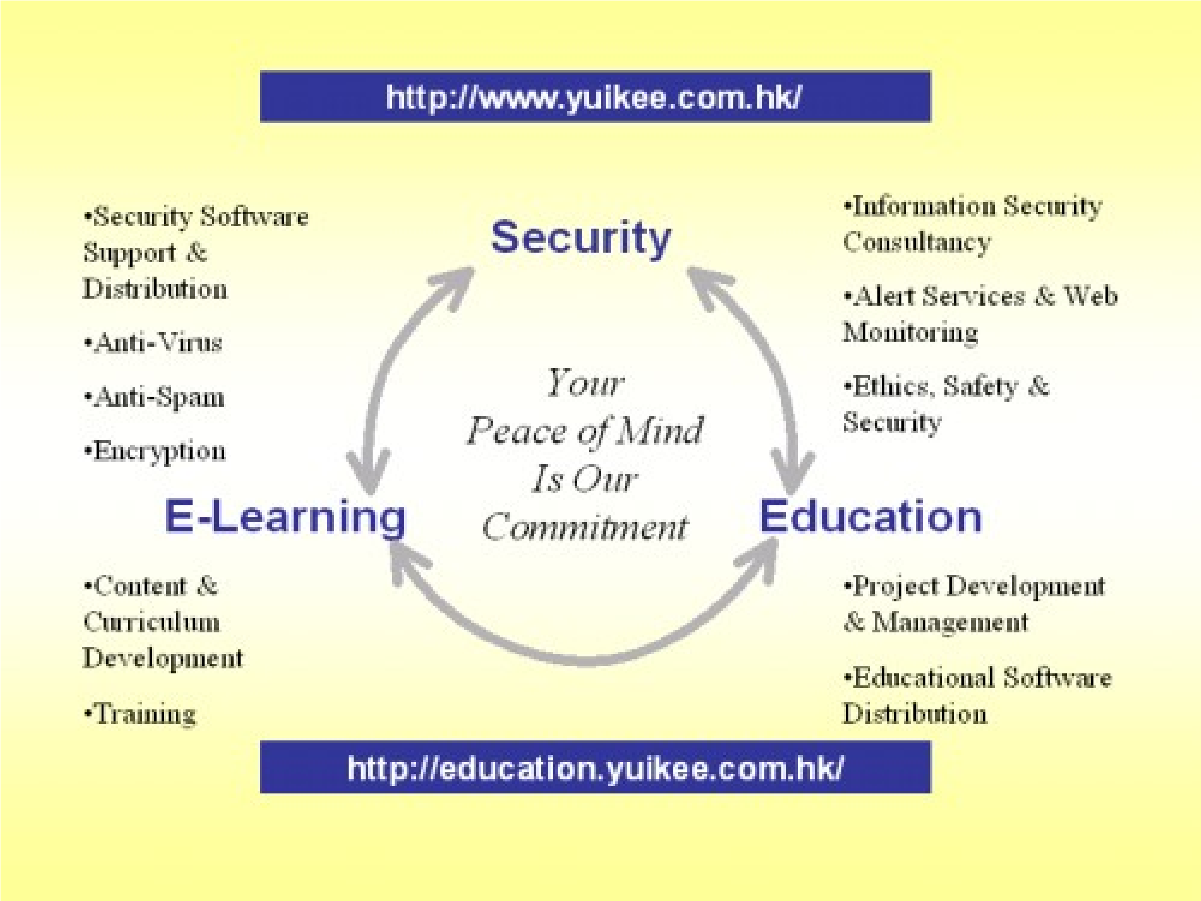
Hazel Poligratis and Augusto Remillano on the ROCKE cryptomining malware.

AVAR 2020 will be held at Ha Long Bay, Vietnam. Since December 2018, Ha Long Bay is served by Van Don International Airport, just 60km away.

Drummers at the Gala Dinner.

YUI KEE
鋭基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

Security

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/