Yui Kee Computing Ltd.

Newsletter

December 2017

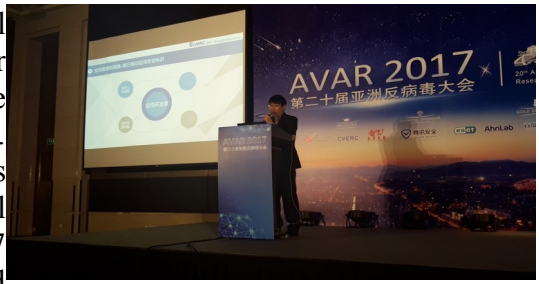
Contents

Contents.....1
At the AVAR 2017 Conference.....1

At the AVAR 2017 Conference

<web-link for this article>

The 20th annual Anti-Virus Asia Researchers (AVAR) Conference was held in Beijing on 6th to 8th December. In his welcoming speech, AVAR Chairman Allan Dyer recounted that the first AVAR Conference was held in 1998, in Hong Kong with just ten participants. Since then, the conference has been held in cities as far North as Tianjin, and as far South as Auckland, New Zealand. It has been to Tokyo, Japan and Chennai, India. This was the sixth conference in China, but the first in Beijing. He emphsised that the AVAR Mission remains the same: To prevent the spread of malware and the damage caused by it.



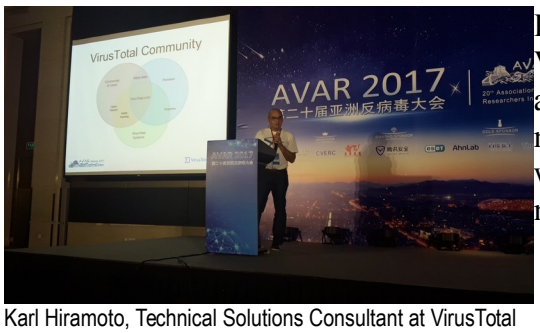
Jianmen Chen, Executive Director of the National Computer Virus Emergency Response Center (CVERC)

Jianmen Chen, Executive Director of the National Computer Virus Emergency Response Center (CVERC) gave a Keynote speech reporting on the work of his center since its establishment in 2011. They have now started protecting mobile apps through the establishment of the China National App Administration Center (CNAAC) on the 17 June 2016. China now has 715 million netizens, and a high percentage are mobile, downloading 90 billion apps. The CNAAC monitors apps in the mobile market looking for terrorism, violence, pornography and rumours in order to maintain social stability. About 95% of the problem apps are malware, including privacy leakage functions and trojans. They have faced challenges in the lack of standards, lack of unified labels for apps and user ignorance, which is a concern because mobile risks affect National Security.

Xi Jinping (习近平) has ordered the creation of a clean internet environment. Since June 2013 he has guided the Ministry of Public Security in improving the national security website, mobile internet security, copyright protection and introducing labels for secure apps through the CNAAC.

Jianmen Chen also said that the CVERC enhanced the coordination of different departments through its conference in Tianjin and it collects statistics for virus infection. They are simplifing the application for app security labels by the use of PKI.

Bin Ma, Vice President of Tencent talked about the trend in the digital economy, big data and artificial intelligence. He emphasised that National Security depends on cyber security and the importance of security fundamentals. He also noted the rise in number of fraudulent phonecalls from fake Police officers.



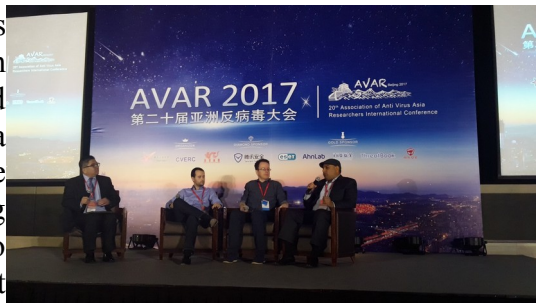
Karl Hiramoto, Technical Solutions Consultant at VirusTotal

Karl Hiramoto, Technical Solutions Consultant at VirusTotal explained the organisation's community approach. VirusTotal was established in 2004 and now includes over 72 scanning engines, thirteen were added during the last year. To be included, a new scanning engine must:

- be 3rd party tested by an AMTSO member
- be capable of scanning selected files and outputting a result of clean, malicious or potentially unwanted application (PUA)
- run on Windows 2012 R2 or Docker
- have average response of ≤3s

They are currently makig a big push on sandboxing.

Jianging Shao, CSO of Microsoft (China) talked about the challenges of the cloud, militarisation and borders in cyberspace. He noted that most malware is seen only once, and advocated Kill Chain Disruption: increasing the cost for attackers, breaking down attack chains and fixing vulnerabilities.



Maik Morgenstern, Bhaarath Venkateswaran, Jesse Song, and Martijn Grooten share a panel on malware testing.

AV-Test CTO Maik Morgenstern, NSS Labs Director of Product Management Bhaarath Venkateswaran, SKD Labs CEO Jesse Song, and Virus Bulletin Editor Martijn Grooten shared a panel on malware testing. They discussed the difficulties of testing and the application of Big Data methods. WannaCry was an opportunity to compare test results to the real world effect, but after 7 months we still have very little information about how effective AV was, or even if it was running on affected systems. Test results are only one part of the AV buying decision. Total Cost of Ownership (TCO) and other considerations have influence. Some testers are already doing IoT security testing, and others are planning to introduce it, but IoT has a vauge definition. It is necessary to go beyond testing products and look at what else works, such as redicing attack surfaces. Bhaarath Venkateswaran reported that there was not much demand for IPv6 product testing; Martijn Grooten noted that IPv6 can easily sneak in unnoticed and Maik Morgenstern agreed that many were using it without realising. Discussing whether cloud-based AV or local AV was best for enterprises, the panelists saw that each had advantages, and it depends on your view on offloading processing or trusting the vendor with the uploaded sample. Martijn Grooten pointed out that data protection regulations might force your choice, and Bhaarath Venkateswaran said that even a locally-processing product might call back to the vendor.

Tiberius Axinte, Technical Leader at Bitdefender gave an in depth analysis of APT28, which has the characteristics of malware produced by a nation-state actor, on macOS. Rowland Yu, Senior Threat Researcher at Sophos covered attacks on Point Of Sale (POS) systems, from traditional magnetic card skimmers to attacks on modern mobile payment systems and QR codes. He noted that the criminals are updating their attack vectors.

Peter Kálnai Malware Researcher at ESET explained his team's efforts in tracking and attributing the Lazarus toolset, produced by a group that has been active for 8 years and which includes WannaCry. He noted suspicious artifacts in the code, such as the name of a South Korean TV series in latinised Chinese, that they considered to be false flags. They also

found evidence of multiple versions of the development environment, indicating that the group spread development over multiple cells.

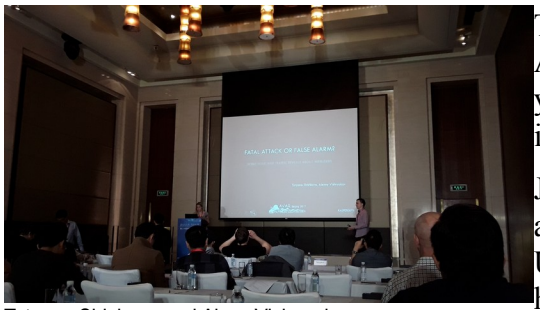
Jin Yang, Senior Security Researcher at Threatbook covered hacking the Bluetooth 4.0 BLE protocol, including BlueBorne, which can take control of devices, the vulnerabilities it is based on and the use of sniffers and custom hardware for protocol attacks.

Eduardo Altares, Senior Threat Analysis Engineer at Symantec described malware-specific markers that can be used to confer immunity to particular threats.

Jacky Cha, Senior Principal Malware Researcher at AhnLab looked at targetted attacks in South Korea and their origin. The Andariel group may be a spinoff of the Lazarus group, but, along with the Operation Red Dot group, their motivation seems to have changed from gathering confidential information to monetary gain. There are at least five of these malware developer groups in South Korea, and some of them are active outside the country.

Filip Kafka, Malware Analyst at ESET reported on FinFisher, which uses a Man In The Middle (MITM) attack at the ISP level to redirect HTTP requests for common installers to a trojanised version. Interestingly, the technique exploited a legitimate product, FinFly, used by ISPs for opt-in parental control. He recommended:

- Don't blindly trust your ISP
- Check the signatures on downloads
- Use HTTPS
- Use a VPN



Tatyana Shiskova and Alexy Vishnyakov

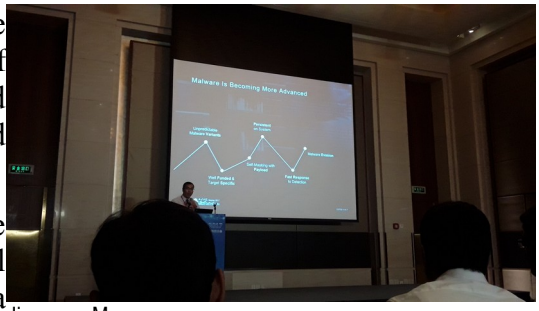
Tatyana Shiskova and Alexy Vishnyakov, Malware Analysts at Kaspersky explained how to examine your web traffic for information about possible infection.

Jingyu Yang, Senior Security Researcher at Tencent, and Fan Dang, PhD Candidate at Tsinghua University, explained their hardware-based IoT honeypot, and the advantages and disadvantages compared to a honeypot in a virtual environment.

Anton Cherepanov and Robert Lipovsky, Senior Malware Researchers at EST, gave a detailed analysis of the biggest threat to industrial control systems since Stuxnet: Industroyer, how it utilises IEC protocols 101, 104 and 61850 and its involvement in the December 2016 Ukraine blackout.

Georgelin Manuel, Software developer at K7 Computing covered detection of advanced Powershell threats using machine learning. Interestingly, the Windows 10 Anti-Malware Script Interface (AMSI) can be bypassed by simply dropping a replacement amsi.dll in the current directory.

Jianpeng Mo, Senior Director of Software Engineering at OPSWAT revealed the rise of Advanced Persistent Threats targetted at the IoT and the challenges of detecting, mitigating and eliminating the threats.



Jianpeng Mo

The conference had two tracks, and many of the speeches are not covered here. The social programme included the welcome drinks, gala dinner with Chinese cultural performers and a local tour. The AVAR 2018 Conference will be held in Goa, India.

More Information

- Association of Anti-Virus Asia Researchers
- AVAR 2017 Beijing
- National Computer Virus Emergency Response Center (CVERC)
- China National App Administration Center (CNAAC)
- International Anti Virus Conference (IAVC) Tianjin
- At the 2017 2nd International Anti-Virus Conference
- VirusTotal

YUI KEE 銳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/