Day-long Media Event

'Microsoft Cyber Trust Experience' Held Successfully in Singapore

Mohammad Abdul Haque Anu

The third edition of 'Microsoft Cyber Trust Experience' was held successfully in Singapore on 21 June, last. The very one-day media event was arranged by Microsoft to enable the company to tell its trust story in Asia. Centered in the Theme of 'Trust', their event focused on discussing the issue of 'Trust' in today's digital world. It is to say, that people will not the technology they do not trust. This is the golden rule that applies to organizations and individuals alike in the mobile-first, cloud-first world. Today we experience constantly growing cyber-attack and cyber-threats, which impact many aspects of our daily lives. Beyond the impact on consumers, as organizations small and large embark on the digital transformation journey, it is critical for them to have steady, consistent approach to security and privacy to maintain and build customer trust.

According to the organizer altogether 15 ICT journalist form 9 Asian countries participated the event. Those who attended the very media event entitled as 'Microsoft Cyber Trust Experience' had the opportunity to get first-hand viewpoints from regional cyber security experts, academics and industry leaders on building and maintaining of trust in a digital world. Other highlights included the launch of a new regional study National University of Singapore (NUS) examining the cyber security risks stemming from non-genuine software and the latest Malware infection index, which identifies the top cyber threats in Asia. The participants also had the opportunity to dive into insights on key cyber security concerns for government organizations and the changing dynamics of the security conversation happening in the boardroom.

Cyber Trust Experience 2017 - Fireside Chat

The Presentation

In this day-long event a number of spokespersons had the presentation on different aspects of cyber trust at different sessions. The first of its kind was on 'Building Trust in a Digital World' presented by Jeff Bullwinkel, Associate General Counsel and Director of Corporate, External and Legal Affairs, Microsoft Asia Pacific and Japan. In this one- hour long session, after the discussion extra 10 minutes was scheduled for questions and answers. During the discussion the speaker tries to make the participants know about, how is trust at the core of everything that Microsoft do. This session was held at Microsoft Transparency and Cyber Security Centre.

There are nearly 400 million victims of cybercrime each year. And cybercrime costs consumers US$113 billion per year.

-Estimates from the Microsoft DCU at Washington DC

Thereafter the second discussion session was held on the same venue and the very topic of discussion was 'Cyber Threat Landscape in Asia'. In this session keynote speaker was Keshav Dhakad, who is the Regional Director, Digital Crime Unit (DCU), Microsoft Asia. In this session he overviewed the cyber threats trends in Asia, including top malware threats and hotspots. At the same time he introduced Microsoft Transparency Centre and Cyber Security center, Digital Crimes Unit and Cyber Threat Intelligent Program to the participants. This 40 ▸

*CTE 2017 - **Jeff Bullwinkel** on A Cloud for Global Good*

*CTE 2017 - **Michael Montoya** on phishing emails*

*CTE 2017 - **Jeffrey Avina** speaking during his session*

*CTE 2017 - **Daryl Pereira** (KPMG) on cybersecurity trends*

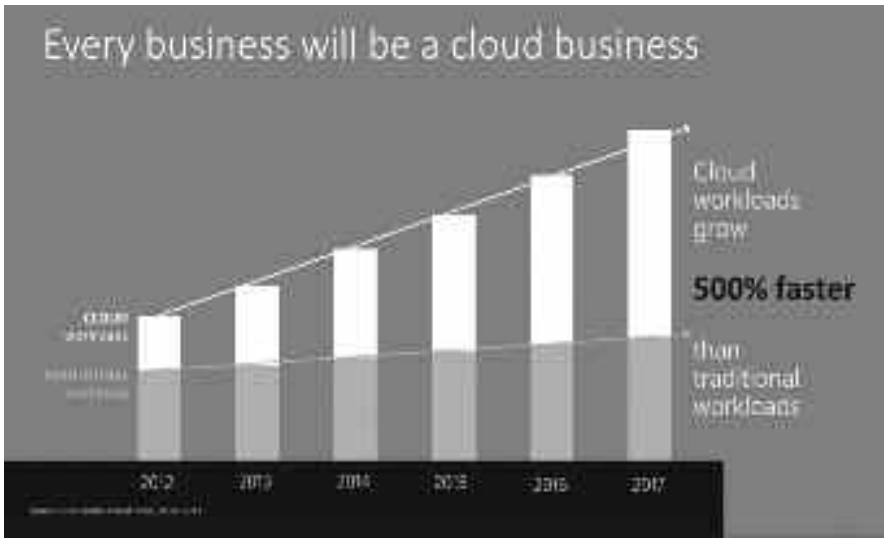
*CTE 2017 - **Keshav Dhakad** on key learnings from cyberattacks*

*CTE 2017 - **Dr Biplab Sikdar** going through the NUS study findings*

minutes long session had no question-answer schedule.

In the third session a joint study on 'Cyber Security Risks from Non-Genuine Software' conducted by Microsoft and National University of Singapore in 2017 was presented. On this issue the key presenters were Keshav Dhakad of Microsoft Asia and Associate Professor Biplab Sikdar of National University of Singapore. The spokesperson highlighted on the key findings of the said study. The participants of the session enjoyed a question and answer session of 20 minutes duration. We like to have thorough look on this study in the later part of this write up under a separate sub-head.

77% of intrusions begin with a **phishing email**



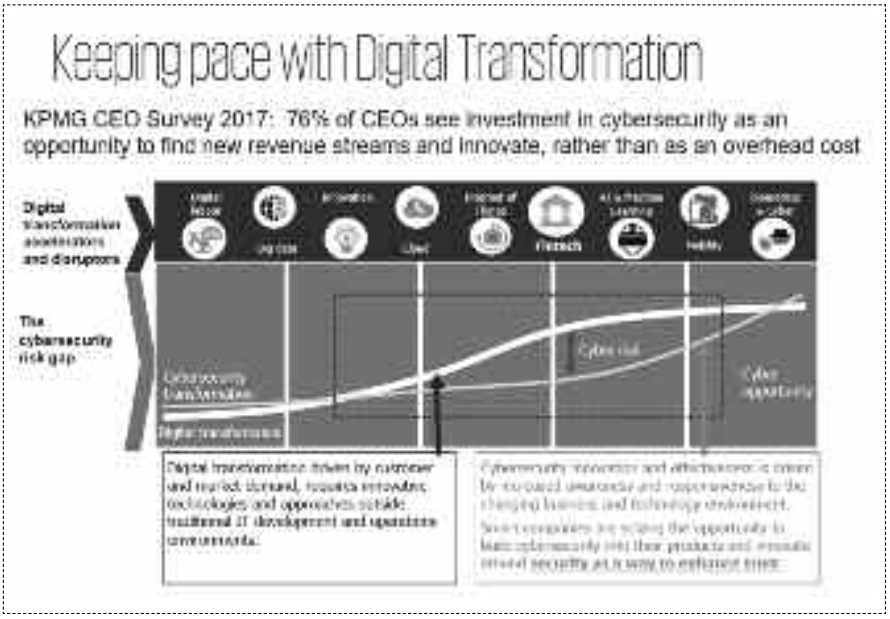
After lunch another one-hour long discussion session on 'Cyber Security Trends and Building a Secure Modern Enterprise' was held, where the key spoke person was Montoya, who is Chief Cyber Security Adviser from Microsoft Asia. In his discussion the issues on which he highlighted included: current threat environment and key challenges that business face; Microsoft's framework for building a Secure Modern Enterprise; introducing the Microsoft Enterprise Cyber Security Group. The session was ended with a question-answer of 10 minutes duration.

The fifth session of one and a half hour duration was on 'Cyber Security in the Boardroom- Changing Dynamics.' The keynote speaker of this session was Daryl Pereira, who is the Head of Cyber security from KPMG in Singapore. In his ▸

presentation he specially focused on trend driving the evolution of cyber security and IT risk management for business in Asia and also on the importance and role of board and senior management in managing IT risk and cyber security.

In the last session the key speaker was Jeffrey Avina, the Regional Director, Government Affairs, of Microsoft Asia Pacific and Japan. His topic of presentation was 'Cyber Security Dialogue in the Governments and National Security. In his discussion he highlighted on two issues: cyber Security trends that are shaping conversations happening on a government-level in Asia; and key concerns and the dangers that cyber attacks pose to countries in the digital era.

Before closing summery there was a Fireside Chat on 'Managing Risks & in the Digital Transformation Journey, where the Moderator was Keshav Dakad. Jeff Bullwinkel, Michael Montoya, Daryl Pereira and Biplab Sikdar participated in this chat.



NUS Study Report

On the day of this event The National University of Singapore (NUS) Faculty of Engineering released the results of its study on, 'Cyber Security Risks from Non-Genuine Software'. The study found that cybercriminals are compromising computers by embedding malware in pirated software and the online channels that offer them. The study was commissioned by Microsoft.

The study, which aims to quantify the link between software piracy and malware infections in Asia Pacific, discovered that 100% of the websites that host pirated software download links expose users to multiple security risks, including advertisements with malicious programs. Among other findings, it also found that 92% of new computers installed with non-genuine software are infected with dangerous malware.

"The study's findings all point to the fact that uncontrolled and malicious sources of pirated software, particularly on the Internet, are being converted into effective means of spreading malware infections. And what we would like to achieve with this report is to help users recognize that the personal and business risks and financial costs are always much higher than any perceived costs they save from using non-genuine software," said Associate Professor Biplab Sikdar from the Department of Electrical & Computer Engineering at NUS Faculty of Engineering, who led the study.

Pirated Software is a Major Source for Malware Infections

Software piracy is a recognized global problem and three in five personal computers (PCs) in Asia Pacific were found to be using non-genuine software in 2016. However, using pirated software expose users to a plethora of cyber threats.

Key Insights from the Cybersecurity Risks from Non-Genuine Software Report

The new study analyzed 90 new laptops and computers as well as 165 software CDs/DVDs with pirated software. The samples were randomly purchased from vendors that are known to sell pirated software from across eight countries in Asia - Malaysia, Indonesia, Thailand, Vietnam, Sri Lanka, Bangladesh, South Korea, and Philippines.

Researchers also examined 203 copies of pirated software downloaded from the Internet. This aligns with the trend where software is increasingly being acquired through online downloads channels. Each of these samples was thoroughly investigated for the presence of malware infections using seven anti-malware engines – AVG AntiVirus, BitDefender Total Security, IKARUS anti.virus, Kaspersky Anti-Virus, McAfee Total Protection, Norton Security Standard, and Windows Defender.

Here are some key insights from the study:

1. Traversing the Malware Minefield – Downloading and Installing Pirated Software from the Internet : One of the most alarming insights from this report is the multitude of risks that users are expose to when they visit websites that offer pirated software downloads. The study found that 100% of tested torrent hosting websites opened with multiple popup windows with suspicious advertisements. Many of these contain links that download malware when clicked or show objectionable content such as pornography.

In addition, the researchers encountered the following risks and suspicious behaviors when downloading and installing pirated software found on peer-to-peer networks:

- 34% of the downloaded pirated software came bundled with malware that infect the computer once the download is complete or when the folder containing the pirated software is opened.
- 31% of the downloaded pirated software did not complete installation which suggests other motives behind their presence on torrent hosting websites. These misleading torrents either tricked users into downloading malicious programs or are used to increase the traffic to the torrent hosting sites which subject the visitor to malware and unwanted advertisements.
- 24% of the malicious programs bundled with the pirated software downloads deactivated the antimalware software running on the computer. Once the anti-malware engine is blocked, the downloaded malware installs itself on the computer.
- 18% of these installations prompt users to change default settings on browsers and install add-on toolbars during installation. These changes to the browser settings lead to new home pages and default search engine as well as unwanted toolbars.
- 12% of these installations require users to contact additional websites to complete the process. This is often portrayed as steps to obtain the license keys or "cracks" needed to activate the pirated software, and they can lead to popups and additional malware exposure.

2. Brand New Computers with Pirated Software – Unused but not Uninfected : The study found that 92% of new and unused computers that had pirated software installed were pre-infected with malware. These computer samples were purchased from vendors that are known to sell non-genuine software.

The presence of malware in these computers is concerning as end-users expect these devices to be risk free. They might be less vigilant in checking for cyber threats and monitoring for suspicious activities that may alert them that their computer has been compromised.

3. Pirated Software in DVDs/CDs – The Classic and Effective Malware Infection Source : Out of the 165 DVDs and CDs samples acquired for this report, three in five (61%) contained malware. Infected discs contained an average of five pieces of malicious programs. In some cases, as many as 38 malware instances were found in just one DVD.

The researchers also observed that a number of pirated anti-virus software were embedded with malware. Using these compromised, non-genuine security programs not only infect the computer, but also lull users into a sense of complacency, which may lead to further exploitation of the computers and the users' data and information.

Types of Malware – Infections Insights

The study found close to 200 malware strains in all the samples. Among those, Trojans were the most common category of high-risk cyber threats encountered, with a total of 79 unique Trojans malware strains. They also comprise 51% of all malware found embedded in downloaded pirated software. While Trojans usually depend on social engineering to trick or mislead users into executing them, bundling them with pirated software make it easier for cybercriminals to compromise PCs. Once a Trojan is active on an infected computer, it installs a backdoor for hackers to access and command the device. This allows cybercriminals to steal confidential information, modify firewall setting, and delete or encrypt data.

An enormous range of worms, viruses and droppers, which were created for stealing information and taking control of their host computers were also found in the samples. These malicious programs can replicate without human intervention and have the capability to spread more rapidly.

Best IT/Cyber-Hygiene Practices for Individuals, Small Businesses and Organizations

Pirated software remains a lucrative revenue stream for many cybercriminals and unscrupulous vendors. The Asia Pacific commercial market of non-genuine software has hit a high of US$19 billion in 20163.

The most effective defense against malware from pirated software is to use genuine software products. Consumers and small businesses can further protect themselves from pirated and counterfeit software as well as malware with the following best practices.

- Source and buy your computers and laptops from reputable vendors.
- Always insist on genuine software from your vendors and opt for computers which come pre-installed with genuine software by hardware manufacturers.
- When purchasing a computer, always request for an invoice which clearly calls out the software title and version which has been installed on the machine.
- Keep your software current with latest product updates and security patches, and strengthen your security posture by having a strong anti-virus software.
- Do not use old operating systems such as Windows XP which have reached their end of life ■