National threat intelligence initiative launched by CyberSecurity Malaysia and Microsoft

AvantiKumar | Nov. 13, 2014

Photo - (Front row from right) YAB. Dato' Seri Diraja Dr Zambry bin Abd. Kadir, Chief Minister of Perak; Keshav Dhakad, Regional Director, IPR & DCU, Microsoft Asia, Legal & Corporate Affairs; YB. Datuk Dr Abu Bakar Mohamad Diah, Deputy Minister, MOSTI and Dr Amirudin Abdul Wahab, Chief Executive Officer, Cybersecurity Malaysia, launching the CTIP activation at CSM-ACE 2014. (Back row, right) General Tan Sri Dato' Seri Panglima Mohd Azumi Mohamed, Chairman, Cybersecurity Malaysia.

A joint Cyber Threat Intelligence Program (CTIP) activation launched by CyberSecurity Malaysia [CSM] and technology solutions giant Microsoft will help governments, network owners and ISPs to provide better online safety for Malaysians.

During the Cyber Security Malaysia Awards, Conference & Exhibition (CSM-ACE) 2014 held in Ipoh, YB Datuk Dr Ewon Ebin, minister of the Science, Technology & Innovation [MOSTI] and YAB Dato' Seri Diraja Dr Zambry bin Abd Kadir, chief minister of Perak presided over the activation of the initiative.

Dr Ewon said "The Malaysian government has always put a high priority on digital development. In fact, the budget allocation for 2015 just on increasing broadband penetration in the country is RM2.7 billion [US$810 million]."

"We can expect to see more Malaysians connected to the digital world in the coming years"," he said. "With more people connected to the internet, the importance of cyber security cannot be over emphasised. It is our collective responsibility to ensure that Malaysians are safe from unscrupulous individuals or criminal organisations who thrive on unsuspecting cyber victims for personal gain."

Microsoft's CTIP collects and distributes actionable cyber threat information, which comprises threat intelligence gathered pursuant to the successful worldwide botnet and malicious software takedown and disruption operations led by Microsoft's Digital Crimes Unit (DCU) and its Cybercrime Centre, headquartered in Redmond, Washington, USA.

CSM's chief executive officer Dr Amirudin Abdul Wahab said: "The role of CSM is to provide specialised cyber security services that contribute towards a key national objective of preventing or minimising disruptions to critical information infrastructure, in order to protect the public, the economy, and government services."

"The data provided by Microsoft's DCU through its CTIP would not only give us valuable insights as to where and how cybercriminals operate and target Malaysians, but would also allow us to act on these findings to protect victims, in our continuing efforts against cybercrime," said Dr Amirudin.

Valuable intelligence

"The CTIP is not a standalone programme," he said "In fact, it cuts across the multitude of initiatives we are currently undertaking. What this means is that Microsoft's CTIP provides data which will allow CSM to extract valuable intelligence for CSM's current initiatives, with insights like malware infestations and new malware threats, which in turn enables CSM to combat the ever evolving landscape of malware, keeping Malaysians safer from cybercriminals."

Keshav Dhakad, regional director, IPR & DCU, Microsoft Asia, Legal & Corporate Affairs, said: "Protecting people is at the forefront of Microsoft's DCU's fight against

SIGN UP FOR OUR E-NEWSLETTERS

RELATED ARTICLES

- U.S. FTC chair wants clearer disclosures to protect privacy
- IT staff not up to speed on EU Data Protection Regulation
- Georgia man sentenced to nine years for stolen credit card data
- Google warns of deadly manual account hijacking attacks
- US putting fake cell towers in planes to spy on people, report says

RELATED WHITEPAPERS

- A revolution in cloud networking
- Faster Oracle performance with IBM FlashSystem
- Are you practising safe BYOD in your organization?
- Stay ahead of malware and cybercriminals
- The Business Value of Identity and Access Management

SEARCH

cybercrime. To date, the DCU has rescued over 65 million IP addresses globally pursuant to our botnet takedown initiatives. With insights from these initiatives, we are able to partner with governments around the world to help protect people, businesses and critical infrastructure."

"In Malaysia, We are thrilled to work with CSM and the Malaysian Government on vital cybersecurity partnerships through CTIP, a global program," said Dhakad. "The CTIP is a powerful big-data resource that allows CSM to have a better situational awareness of existing cyber threats and potential malware related security issues in Malaysia. CSM can then leverage the real-time cyber threat intelligence gathered through CTIP to keep up with the fast-paced and ever-changing cybercrime landscape, and work with consumers and businesses to help them eliminate these threats from their machines and IT environments."

"Organisations like CSM and the DCU have the tools and resources to fight cybercrime, but the biggest impact comes from awareness and prevention," he said. "Consumers and businesses need to be aware of how malware infects through poor Internet practices and unsecure supply chain, such as usage of non-genuine software, and the proactive steps that can be taken to ensure that they are safe online. A genuine and trusted software ecosystem is far more agile and protected against cyber-threats."

Two basic attack strategies

"Cybercriminals use two basic strategies to penetrate your computer's defences and enlist computers in their botnets for malicious purposes," said Dhakad. "Firstly, they install malware on a computer by taking advantage of pirated or counterfeit software, or secondly, by breaking into accounts guarded by weak passwords or by taking advantage of poor Internet and IT practices."

"In fact, earlier this year, a National University & Singapore (NUS) and IDC Cybersecurity Research showed that of 203 new PCs purchased in 11 countries with counterfeit software installed on them, 61 percent of those PCs were pre-infected with malware," he said.

Dhakad said malware infected PCs posed significant risks to both consumers and businesses. The NUS and IDC study estimated that consumers will spend nearly US$25 billion and waste 1.2 billion hours dealing with security issues created by malware on counterfeit software, whereas enterprises will spend US$491 billion dealing with security issues and data breaches in 2014.

"Malware loaded onto counterfeit software infects and steals information from a victim's computer," he said. "Cybercriminals are then able to use that information to illegally enter and abuse the victim's online services, including online bank accounts, email systems, and social networking sites.

This can have damaging effects on users' financial security and personal safety, as well as pose a risk of corporate espionage and surveillance."

CSM's Dr Amirudin said Malaysian consumers and businesses needed to be more proactive in combatting malware. "We would like to urge Malaysians to regard cybersecurity as their first priority and they must know how to protect themselves from malware and other computer viruses by insisting on genuine software when purchasing computers."

"Using a computer with counterfeit software is just like opening doors to cybercriminals. People and businesses who use counterfeit software have no guarantee that their personal, confidential, sensitive data, activities and communications online using these devices, will be safe from cybercriminals that intend to do harm," he said.

Customers who suspect they've received pirated or counterfeit software are encouraged to report it at microsoft.com/piracy

COMMENTS

CIO ASIA

Sophos CEO: We're betting entirely on the cloud

What CIOs can learn from the biggest data breaches

Halfords CIO: Moving to managed cloud SAP service enabled business to create new service

Facebook, LinkedIn and Twitter earnings tell very different tales

Forrester's 2015 predictions: Mobile customer experience will fuel digital transformation in Asia Pacific

MIS ASIA

THE HOME OF ENTERPRISE IT IN ASIA

Hong Kong workers demand an ideal workplace

Alibaba rakes in US$9.3B as Chinese splurge online during Singles' Day

China's e-commerce binge tests logistics, rakes in sales

North Korea reportedly blocks Facebook and Twitter

Baidu traffic from mobile devices now more than from PCs

COMPUTERWORLD SINGAPORE

Bank of Singapore hires Bahren Shaari as its new CEO

Companies in Singapore satisfied with Big data outcomes: Accenture Study

StarHub voice and data services fully restored after 8-hour outage

Singapore data centre budgets to grow

Microsoft Singapore partners ITE to offer one-to-one learning