Sophos to place Spotlight on synchronized security at GISEC 2017

DUBAI: Sophos (LSE:SOPH),a global leader in network and endpoint security announced its participation at Gulf Information Security Expo & Conference (GISEC 2017) which will be held from May 21st - May 23rd, 2017 at the Dubai World Trade and Convention Centre. The company will showcase its extensive security portfolio and focus on its synchronized security strategy.

"Given the scale and sophistication of attacks in the Middle East region, companies are looking for smarter and simpler IT security solutions. A recent Sophos-sponsored study developed by International Data Corporation (IDC) revealed that complexity is driving the need of integrated security in the region and it is one of the top priorities for CIOs and IT Managers. Majority of the respondents agreed with the concept of linking network firewall and endpoint security for better insights and the acceptance was higher among the large enterprises. Synchronized security is the new key for protection against cyber threats in the region," said Harish Chib, VP MEA Sophos.

"GISEC, being an important event for the Middle East IT security industry, is a perfect platform for Sophos to communicate our vision of 'Synchronized Security'. We plan to highlight our latest innovation, Security Heartbeat, which for the first time allows the endpoint and network security to actively and continuously share threat intelligence to effectively protect against sophisticated threats in a manageable way. It is also a great opportunity for us to meet with key decision makers." he added.

Harish Chib, Sophos

At the exhibition, Sophos will highlight the core tenant of synchronized security strategy that can be used to successfully protect an organization from the growth of sophisticated attacks. The company will showcase its extensive portfolio of its next-generation endpoint and network security solutions including the recently launched Sophos Mobile 7, the latest version of Enterprise Mobility Management (EMM) solution that extends containerization support for Android Enterprise, Sophos InterceptX, and the latest synchronized encryption solution -Safe Guard Encryption8, which can automatically respond to threat incidents from connected endpoint protection.

Sophos top local executives and security experts will be present at Stall B-100,Hall : ZAB5 and will engage with visitors, customers and channel partners, understand their security requirements, address their concerns and share their global experiences and success stories with them. Through presentations and demos at the stand, the company plans to give its customers a firsthand experience on the benefits of synchronized security.

This file photo taken on July 21, 2014 shows an employee of Equinix data center checking servers on July 21, 2014 in Pantin, a suburb north of Paris in the Seine-Saint-Denis department. —AFP

Worldwide ransomware attacks: What we know

LONDON: Security agencies are hunting for those behind a crippling cyberattack which has so far hit hundreds of thousands of computers worldwide, including at government agencies, factories and health services. Here is what we know so far about the cyber ransom attacks:

*** What happened?**

The cyberattacks started Friday and spread rapidly around the globe using a security flaw in Microsoft's Windows XP operating system, an older version that is no longer given mainstream tech support by the US giant. The so-called WannaCry ransomware locks access to user files and in an on-screen message demands payment of $300 (275 euros) in the virtual currency Bitcoin in order to decrypt the files.

Victims have been advised by security experts not to pay up. The attack is unique, according to policing agency Europol, because it combines ransomware with a worm function, meaning once one machine is infected, the entire internal network is scanned and other vulnerable machines are infected.

*** Who has been affected?**

Europol chief Rob Wainwright said computer systems in more than 150 countries were hit, with the majority of organizations affected over the weekend in Europe. But as Asia woke up to the working week yesterday, leading Chinese security-software provider Qihoo 360 said "hundreds of thousands" of computers in the country were hit at nearly 30,000 institutions including government agencies.

In Japan, a spokesman for Hitachi said the conglomerate discovered problems on Monday morning and its computer networks were "unstable". Other high-profile victims include hospitals in Britain, the Spanish telecoms giant Telefonica, French carmaker Renault, US package delivery company FedEx, Russia's interior ministry and the German rail operator Deutsche Bahn.

*** Where did the malware come from?**

Brad Smith, Microsoft's president and chief legal officer, said in a blog post Sunday that the culprits used a code developed by the US National Security Agency.

It was leaked as part of a document dump, according to researchers at the Moscow-based computer security firm Kaspersky Lab. Smith warned governments against stockpiling such vulnerabilities and said instead they should report them to manufacturers-not sell, store or exploit them, lest they fall into the wrong hands.

"An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen," Smith wrote. "The governments of the world should treat this attack as a wakeup call."

*** Who was behind the attack?**

Europol said yesterday it was continuing to hunt for the culprits behind the unprecedented attack.

The agency's senior spokesman Jan Op Gen Oorth said it was still "a bit early to say who is behind it, but we are working on a decrypting tool".

Experts think it unlikely to have been one person, with criminally minded cybercrime syndicates nowadays going underground and using ever more sophisticated encryption to hide their activities.

*** How can people protect their computers?**

Microsoft took the unusual step of reissuing security patches first made available in March for Windows XP and other older versions of its operating system. Kaspersky said it was seeking to develop a decryption tool "as soon as possible". Europol said European companies and governments had heeded warnings and as a result avoided further fallout from the ransomware.

"It seems that a lot of internet security guys over the weekend did their homework and ran the security software updates," Jan Op Gen Oorth said.—AFP

Tech Mahindra ranked amongst top 15 global tech services brand

Brand value grows 21% fuelled by its DT initiatives

DUBAI: Tech Mahindra, a specialist in Digital Transformation, Consulting, Services and Business Re-engineering and Brand Finance, the world's foremost independent branded business valuation consultancy announced Tech Mahindra's entry into the Top-20 global tech services brands list (by brand value) in 2017, ranked at No 14, with an impressive growth of 21 percent over the previous fiscal.

Brand Finance is an independent valuation and strategy consultancy. It advises organizations on how to maximize value through effective management of brands and other intangible assets and is world-renowned for its pioneering work in brand valuation. Brand Finance helped to shape the internationally recognized standard for brand valuation, ISO 10668, and is one of just a select group of firms to hold the certification. Brand Finance was founded in London 1996 and now has offices in over 25 countries.

Underscoring this achievement, David Haigh, Founder and CEO of Brand Finance commented, "Tech Mahindra has delivered excellent brand value growth of 21 percent. Its brand transformation journey from being an Information Technology player to a Digital Transformation partner has shown great progress. With its new brand promise of 'Connected World, Connected Experiences' and the right brand investments, Tech Mahindra has all the potential to be in the top 5 by 2020." Tech Mahindra has recently embarked on a massive brand building campaign globally forging strategic partnerships with several Global Media Groups, local Governments and Trade Councils, to bring alive its "Connected World. Connected Experiences." promise. The Company aspires to consolidate and improve its position through significant brand investments aligned to its core strategy in delivering tangible "experience" outcomes to its 900+ customers worldwide. The Company's Techbets will deliver DIGITALISATION, AUTOMATION, VERTICALISATION, INNOVATION and DISRUPTION (#DAVID), readying its customers to face the digital future with products, platforms, design, experience and knowledge.

Jagdish Mitra

Celebrating this moment, Jagdish Mitra, Chief Marketing and Strategy Officer of Tech Mahindra said, "We are immensely glad to have entered the veritable brand club and would like to thank our associates, partners and customers, for helping place our brand where it deserves to be. We have embraced Digital Transformation as the bedrock of our brand journey, at a time when connectedness and experiences are the fundamentals for any business and consumer across all aspects of daily living. Our brand will constantly endeavour to reflect this, as we Run better, Change faster and Grow greater for our stakeholders."

For some ransomware victims, hard lessons

SINGAPORE/HANOI: The WannaCry ransomware worm that hobbled big institutions and businesses at the weekend, including FedEx and Britain's National Health Service, also indiscriminately caught many smaller victims across Asia, from hoteliers to Chinese students.

When MediaOnline, a firm that operates digital displays in Singapore shopping malls, noticed its displays were showing the ransomware's pop-up window on Saturday, it sent engineers to two malls, director Dennis So told Reuters.

The company's experience shows how the ransomware can sometimes be beaten without victims having to pay the $300 or so in bitcoin that hackers demand for a decryption key to unfreeze their computers. MediaOnline's So said only 12 computers were affected as the network was isolated from both the firm's office network and those of the company running the malls, and its tenants. By replacing all the hard drives, reinstalling the operating system and downloading all Microsoft Windows updates, the computers were back up and running by early Monday, with So saying "no money or bitcoin was paid to the hackers."

At some larger organizations, it took longer. At Jakarta's Dharmais Hospital, Indonesia's biggest cancer centre, up to 200 people packed waiting rooms after cyberattacks hit scores of computers. By late yesterday morning, some visitors were still filling out forms manually, though the hospital said 70 percent of its systems were back online.

The unknown hackers behind WannaCry don't appear so far to have been well rewarded for their global blitz, with about $50,000 worth of bitcoin transferred to the online wallets listed in the recent and earlier versions of the malware, according to bitcoin transaction tracker Elliptic Labs.

This may be partly because many of those infected, like MediaOnline, chose to restore their computer data from back-ups or by reinstalling the operating system. Others just held their breath.

Lost work

Yang Lin, a journalism student at China's Zhejiang University of Media and Communications, told Reuters she had just finished revising her thesis late on Friday and was closing Word on her desktop when all the Word icons blanked out, her screen went black and the hackers' message appeared. "I was connected to the university network. I didn't open any link," she said. "I just cried. I was afraid to believe it, but had to accept it."

Yang said she thought about paying the ransom to unfreeze her computer, but gave up when she found out how much this would cost. Via a chat platform she discovered many of her friends faced the same problem. She said she lost her literature review, foreign translations and thesis proposal, as well as films she had made over four years at college.

In Vietnam, hotel and restaurant manager Ngo Viet Yen said he was given 24 hours to pay 5 bitcoins (worth around $9,000) to save his files after his systems were infected on Friday. He didn't pay, and reckons he's lost around $2,000, and possibly more, as his staff revert to taking bookings, writing receipts and managing stock manually.

He noted that copyright infringement is widespread in Vietnam, and little is spent on system security. "The number of computers updated to the latest version is very low," he said. "And the server is rarely updated because there will be more issues and it often slows the system. It's like: you only build a cage after losing your cows."

Others found that even paying the ransom didn't guarantee they'd get their data decrypted. "We've seen some of our customers from the energy and health services who made the payment did not receive the decryption key in return," said Budiman Tsjin, senior technical consultant at RSA, the security division of EMC Corp. —Reuters

JAKARTA: A patient takes a nap on her wheelchair as she waits with others at the registration desk at Dharmais Cancer Hospital in Jakarta yesterday. Global cyber chaos was spreading yesterday as companies booted up computers at work following the weekend's worldwide "ransomware" cyberattack. —AP

40% of industrial computers faced cyberattack: Kaspersky

DUBAI: Kaspersky Lab is participating in the 2nd ISA UAE Automation Conference and Exhibition 2017 in Abu Dhabi to share its expertise on cybersecurity of industrial control systems (ICS).

The percentage of industrial computers under attack grew from over 17 percent in July 2016 to more than 24 percent in December 2016, with the top three sources of infection being the Internet, removable storage devices, and malicious e-mail attachments and scripts embedded in the body of e-mails. On average two-in-five computers, related to the technological infrastructure of industrial enterprises, faced cyberattacks in the second half of 2016. These are the findings from Kaspersky Lab's report, the "Threat Landscape for Industrial Automation Systems in the second half of 2016."

As the technology and corporate networks of industrial enterprises become increasingly integrated, more and more cybercriminals are turning their attention to industrial enterprises as potential targets. By exploiting vulnerabilities in the networks and software used by these enterprises, attackers could steal information related to the production process or even bring down manufacturing operations, leading to technogenic disaster.

In order to find out how widespread the threat is, Kaspersky Lab ICS CERT specialists have conducted dedicated research into the cyberthreat landscape faced by ICS systems.

They discovered that in the second half of 2016 malware downloads and access to phishing web-pages were blocked on over 22 percent of industrial computers. This means that almost every fifth machine at least once faced the risk of infection or credential compromise via the Internet.

The desktop computers of engineers and operators working directly with ICS do not usually have direct access to the Internet due to the limitations of the technology network in which they are located. However, there are other users that have simultaneous access to the Internet and ICS. According to Kaspersky Lab research, these computers - presumably used by system and network administrators, developers and integrators of industrial automation systems and third party contractors who connect to technology networks directly or remotely - can freely connect to the Internet because they are not tied to only one industrial network with its inherent limitations.

Trade groups appeal to Beijing to postpone cybersecurity law

BEIJING: A coalition of 54 global business groups appealed to Chinese authorities yesterday to postpone enforcing a cybersecurity law they warned violates Beijing's free-trade pledges and might harm information security.

The appeal by groups from the United States, Japan, Britain and other countries adds to complaints Beijing is improperly limiting access to its markets for technology products, possibly to support its own fledgling suppliers. In a letter to Chinese regulators and the ruling Communist Party's cybersecurity committee, the groups said the Cybersecurity Law due to take effect June 1 might violate Beijing's trade commitments and make theft of information easier. It would limit use of foreign security technology and require data about Chinese citizens to be stored within the country.

Signers included the Business Software Alliance, the US Chamber of Commerce and trade groups for insurers, technology suppliers and manufacturers from Britain, Japan, Australia, Mexico and South Korea. Many of them were among 46 groups that made a similar appeal in 2016 for changes in the cybersecurity law, which weren't made. —AP