AMCHAM

SRI LANKA

AmCham Sri Lanka Knowledge Hub Series: The Bulletin Board – Topic-in-Focus

THE AMERICAN CHAMBER OF COMMERCE IN SRI LANKA

The American Chamber of Commerce in Sri Lanka (AmCham SL), is one of the most influential and prestigious business chambers in the island, recognized as *the* forum for the facilitation and development of trade, investment and business relations between Sri Lanka and the United States.

The AmCham SL is an Association whose stakeholders are its over 350 members, made up of top blue-chip organizations in the island and provides its members a multi-dimensional resource network that delivers information, tools and knowledge they need to succeed in bilateral business relations between the two Nations through information share, LQAs, Seminars, Workshops, B2G and B2B networking and exclusive connect & advisory services.

AmCham SL may be contacted at | ed@amcham.lk

© AmChamSL|2020

Hacking isn't canceled nor are Hackers in lockdown

By Sujit Christy

The novel coronavirus spread is continuing to affect hundreds and thousands of people around the world. From cancelled conferences, sporting events to disrupted international travel and supply chains, not a corner of the global economy is immune to the spread of COVID-19. The pandemic is different stages in various countries and the decision on measures taken by the governments are based on local situations and the progression of the disease.

The economic challenges caused by this pandemic is unprecedented. The pandemic exposed the risky dependence on vulnerable nodes in supply chains. The government and business leaders have found ways to safeguard lives and livelihoods. Many organizations implemented basic protections for their employees and customers and resumed activities in a limited way. This included "no-travel" and "work-from-home" policies for workers and physical-distancing-at-work for others in essential and frontline services until the countries are in a position to battle and control resurgence.

Everything that could be moved online from entire company workforce to workflows to shareholder meetings, schools to university classes, public service, wellness and social practices has been moved. Platforms like Zoom, Google Hangouts and Houseparty integrated into workflows and social hours across the world, and the same technology is now among high-demand features of the dating world: video and audio dates. This has propelled the adoption of new technology across all aspects of life thus emerging to become a permanent fixture of the next normal. These are the business cases for more advanced and robust 5G technologies for a future business, health care and human interaction to be at more than an arm's length.

Engagement via voice, text and image is taking the place of human-to-human interaction. Being connected is the one thing people desire right now. In order to be connected, users rely on their home broadband networks or mobile connectivity to interact with their organizations and outside world. This has prompted a surge in cyberattacks including phishing scams and spam over the past three weeks as the hackers have realized the users are now working outside of their fortified corporate network.

Disclaimer: The views, opinions and/or analysis expressed in this article are those of the author and do not necessarily reflect the views, opinion and/or official policy or position of the American Chamber of Commerce in Sri Lanka.

© AmCham Sri Lanka Publication/2020

The cybercriminals and unscrupulous marketers have taken advantage and have seized upon concerns and anxiety over the emergence of the coronavirus pandemic as bait for spam, phishing attacks and malware to attack the remote workforces, customers, suppliers and corporate systems.

The hackers know that every IT department and cybersecurity teams are currently overwhelmed, stretched and are less able to respond in the current situation.

Potentially unwanted email messages, and phishing and malware delivery schemes are using the domain names "coronavirus" and "COVID-19". Since January 2020, over 16,000 new coronavirus-related domains have been registered and about 2,200 were found to be suspicious and 93 were confirmed as malicious and dangerous to visitors.

Further, the coronavirus tracker apps that claim to let people see if there have been outbreaks in their area but instead infect devices with malware to deliver ransomware to endpoint devices and seize control of the device and the corporate systems. The emails purporting to be from IT Departments, email service providers, popular web sites or video conferencing services such as Zoom and Microsoft Teams, lure people to change passwords or update security and privacy settings has also increased.

The sextortion or porn scam email claiming to have implanted malware on device to monitor and track online activity has also been on the increase.

Adult sites are one of the top categories of websites hosting malicious content and a favorite tool of the hackers. Users watching porn from the corporate owned device or personally owned device which used to connect to the corporate network during coronavirus lockdown leaves companies open to cyberhackers. It may be more effective if a user of an organization decide that what is typically not safe for work (NSFW), that it is safe for working from home during the coronavirus outbreak. The hackers are targeting organizations and are seizing on this opportunity to hold on to anything for ransom or sell information to a competitor.

Disclaimer: The views, opinions and/or analysis expressed in this article are those of the author and do not necessarily reflect the views, opinion and/or official policy or position of the American Chamber of Commerce in Sri Lanka.

© AmCham Sri Lanka Publication/2020

As organizations transform digitally and adopt remote working, it is time for them to validate their existing cybersecurity architecture besides developing a governance framework for remote working. There's no perfect defense against hacks, but users can lower their risk by practicing "digital hygiene." The following are some good digital hygiene the users should adopt:

1. Passwords: Use different passwords for different corporate applications and personal applications. Password should be complex, changed frequently and should never be shared with others. Where possible, the users should enable the two-factor authentication.

2. Wi-Fi: Change the default passwords in the Home wi-fi routers. Enabling appropriate encryption methods. Where wi-fi networks are not available, the users should enable their mobile hotspots with strong passphrases. Never connect to an unknown wi-fi network.

3. Updates: Operating Systems in the laptops and desktops should be configured to patch directly from the internet. Patches should always be up to date.

4. Antivirus: Use a reliable commercial antivirus in the laptops, Desktops and Mobile devices. Antivirus signatures should be up to date and firewalls in the end points should be enabled and the storage encrypted.

5. Data Classification: Identify sensitive and educate users to handle them carefully. Adopt a data classification tool to classify data to minimize the risk of accidental disclosure.

6. Backup: Data should be always be backed up to a secure location. This will minimize the risk of data loss due to loss of hardware or failure.

7. Secure Remote Access: The administrators should use a good commercial and reliable VPN client to connect securely to the corporate network. All VPN clients should be multi-factor authentication enabled. Adopt Virtual Desktop Infrastructure (VDI) for the end users to access corporate applications and data. Free Mobile VPNs should be avoided as they terminate in servers that propagate malware.

8. Cybersecurity Awareness: As part of the work-from-home guidance, continue to encourage users to be vigilant and exercise extreme caution when clicking outbound links or attachments, reminding them of the ransomware attacks that have hit so many organizations both in Sri Lanka and in other countries.

Disclaimer: The views, opinions and/or analysis expressed in this article are those of the author and do not necessarily reflect the views, opinion and/or official policy or position of the American Chamber of Commerce in Sri Lanka.

© AmCham Sri Lanka Publication/2020

While adopting the good hygiene, the users should also be careful in sharing personal information including private pictures and videos. As for organizations, they should continuously monitor their infrastructure and assess the controls implemented are effective and works as intended.

The writer is a Cybersecurity professional and Director at Layers-7 Seguro Consultoria (Pvt) Ltd. He is a board member of the ISACA Sri Lanka Chapter.

He is the Founder/President of Information Security Professional Associates (iSPA). He is the founding member and Past President/Secretary of the (ISC)² Chennai Chapter and past board member of (ISC)² Colombo Chapter. He can be emailed at sujit@layers-7.com

Disclaimer: The views, opinions and/or analysis expressed in this article are those of the author and do not necessarily reflect the views, opinion and/or official policy or position of the American Chamber of Commerce in Sri Lanka.

© AmCham Sri Lanka Publication/2020