TODAY DAY IN HISTORY

1934

Bill Wilson, co-founder of Alcoholics Anonymous, takes his last drink and enters treatment for the last time.

1941

World War II: Poland declares war on the Empire of Japan.

1941

World War II: The Imperial Japanese Navy suffers its first loss of surface vessels during the Battle of Wake Island.

1946

The United Nations International Children's Emergency Fund (UNICEF) is established.

Flawless phishes, monetisation and intelligence: What's ahead for cybersecurity in 2019?

The World Economic Forum recently placed cybersecurity as the fifth biggest global risk for doing business

BRIAN PINNOCK

What lies ahead for companies, governments and individuals regarding cybersecurity in 2019? Will we see the EU government forcing US data centers to hand over data? Will the European Union issue its first major fines for organisations in contravention of its General Data Protection Regulation? Will our growing dependence on social media expose us to unwanted risks as our accounts become compromised?

The World Economic Forum recently placed cybersecurity as the fifth biggest global risk for doing business, with 19 countries ranking it as their number one concern, including 14 in Europe and North America, as well as Japan, India, Indonesia, Singapore and the UAE. As the political climate around the world continues to create volatility, growing numbers of connected global citizens will turn to the Internet to have their message heard. The growth in connected devices– from consumer wearables to industrial IoT to medical devices – is compounding the security challenge as each device represents a potential cybersecurity risk.

Here, we take a global look at some of the key developments we expect to see on the cybersecurity front in 2019.

More effective, not different, cyberattack types

Throughout 2019, the most insidious development won't be new attack types but rather improved execution of existing attack types, especially those delivered via email. Better social engineering, more advanced phishing attacks, increases in credential stuffing attacks, and more complicated malware with multiple stages and different form factors for transmission, will make threats incredibly tricky to detect.

Phishing techniques like the use of homoglyphs, elongated URLs, the use of legitimate certifications (green lock), and credential-harvesting sites will increase. Flawless phishes will continue to prey on the gap in human firewalls, pivoting internally around organisations and intensifying efforts to better educate all staff. Cybersecurity awareness training, which according to a global Mimecast and Vanson Bourne study is only continuously conducted by 11% of global organisations, will receive renewed attention as organisations bolster the capabilities of their first line of defence: their employees.

Cybercriminals will also shift focus to weaker countries and industry verticals that lag in their adoption of more advanced cyber defences. More industrialised countries are investing heavily in cybersecurity, making them less attractive to cybercriminals. Companies in particularly the Middle East and Africa often assume their security is sufficient without realising that the threat landscape is drastically shifting. This makes them easy targets for cybercriminals who tend to follow the path of least resistance. Attackers will also continue to shift their attention away from larger organisations to small and medium businesses.

Cybercriminals will also shift focus to weaker countries and industry verticals that lag in their adoption of more advanced cyber defences.

Monetisation of data breaches

There have been several highly successful high-profile data breaches over the past few years. From Equifax to Facebook, eBay to JPMorgan, hackers have made off with sensitive data for hundreds of millions of user accounts. Just recently, Marriott announced that its Starwood database was hacked for approximately 500 million guests – one of the largest breaches in history. With global cybercrime organisations' growing in maturity and sophistication, many are now acquiring capabilities that were once the sole reserve of nation states. We're likely to see these cybercriminals use stolen credentials from the past few years' data breaches to compromise the security of even the most secure organisations. Even companies with good cyber protection have little protection against the reuse of passwords that have been collected in other breaches.

The evolution of cyberattacks has also created entire ecosystems of fraud. Stolen personal health information, for example, could be used to gain insight to patients' ailments and likely treatments. Hackers could use this information to obtain prescriptions for strictly controlled medication that is then traded or sold illegally. It's no longer just about a straightforward cyberattack: cybercrime is fast becoming a trickle-down economic system with multiple layers of fraud and criminality built into its very fabric.

Intelligence becomes 'intelligent'

Organisations will realise the importance of threat intelligence and will talk about the need for an intelligence function. What they really mean is that they want some insight from their vendors around the huge amounts of threat data they're acquiring. There may be a handful organisations who will stop recasting threat data as intelligence and instead focus on generating actionable insights from this data, the prerequisite for 'threat intelligence'. Unfortunately, the vast majority still won't take any action from the data presented, which means they won't actually have any intelligence –only an interesting storyline.

Artificial intelligence and machine learning will play a more prominent role as the velocity and variety of attacks makes conventional approaches – such as blacklists – outdated and ill-equipped to deal with modern cyber threats. The average phishing site, for example, is only online for a few hours. With such a crowded domain space, attackers have to be clever about the domains they register and exploit. Luckily, these domains generally have certain characteristics, which machine learning algorithms can exploit and detect, while other properties of attack vectors can also be recognised by appropriately trained AI.

AI will also be used to detect break-ins, spam, phishing and more. Although it will mostly work well, look out for the occasional mistake: these will be utterly incomprehensible to humans, and very hard for vendors to explain to their customers.

From financial gain to life-and-death

As our world becomes increasingly digitised and connected devices continue to permeate every aspect of our daily lives, the risks posed by cybercriminals are escalating. A large-scale attack on critical infrastructure such as energy services, water supplies or even hospitals could cause massive damage and even loss of life. Autonomous vehicles, although not prevalent on our shores yet, are attractive targets for the more ruthless type of cybercriminal. And with the growth in digital medical devices, hackers could directly target an individual and interfere with their pacemakers or heartrate monitors.

Privacy will also become a key concern: consumer connected devices such as cameras, microphones and wearables will become a major security issue as hackers discover ways to see live audio and video of unsuspecting people's lives. The fallout of such an incident being exposed could drastically erode trust in technology and make people treat technology with greater caution as they realise the devices they have enjoyed without concern, carry immense risk to their personal privacy and security.

Even though the threat landscape keeps changing what seems to be the common thread is that email continues to be the most common - and least protected - attack vector. We can't predict exactly what 2019 threats will look like, but we can predict that while email remains vulnerable it will continue to be the preferred entry point for criminals to deliver threats to your organisation.

(Brian Pinnock is a cybersecurity specialist at Mimecast.)

TOP 4 TWEETS

01

"Democrats can't find a Smocking Gun tying the Trump campaign to Russia after James Comey's testimony. No Smocking Gun...No Collusion." @FoxNews That's because there was NO COLLUSION. So now the Dems go to a simple private transaction, wrongly call it a campaign contribution,...

@realDonaldTrump

02

Love, kindness, compassion and tolerance are qualities common to all the great religions, and whether or not we follow any particular religious tradition, the benefits of love and kindness are obvious to anyone.

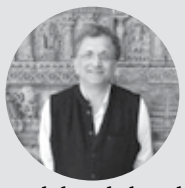
@DalaiLama

03

Dr. Urjit Patel is a thorough professional with impeccable integrity. He has been in the Reserve Bank of India for about 6 years as Deputy Governor and Governor. He leaves behind a great legacy. We will miss him immensely.

@narendramodi

04



I have deleted the photo of my lunch in Goa as it was in poor taste. I do wish however to again highlight the absolute hypocrisy of the BJP in the matter of beef, and to reiterate my own belief that humans must have the right to eat, dress, and fall in love as they choose.

@Ram_Guha

Disclaimer: (Views expressed by columnists are personal and need not necessarily reflect our editorial stances)

nikrishnan | **Advertisement**: Update Media W.L.L | Tel: 38444692, Email: sales@newsofbahrain.com | **Newsroom**: Tel: 38444680, Email: mail@newsofbahrain.com
in.com | Website: www.newsofbahrain.com | Printed and published by Al Ayam Publishing