How hackers are utilizing coronavirus to prey on human fears

(Image source: Internet photo).

Overview

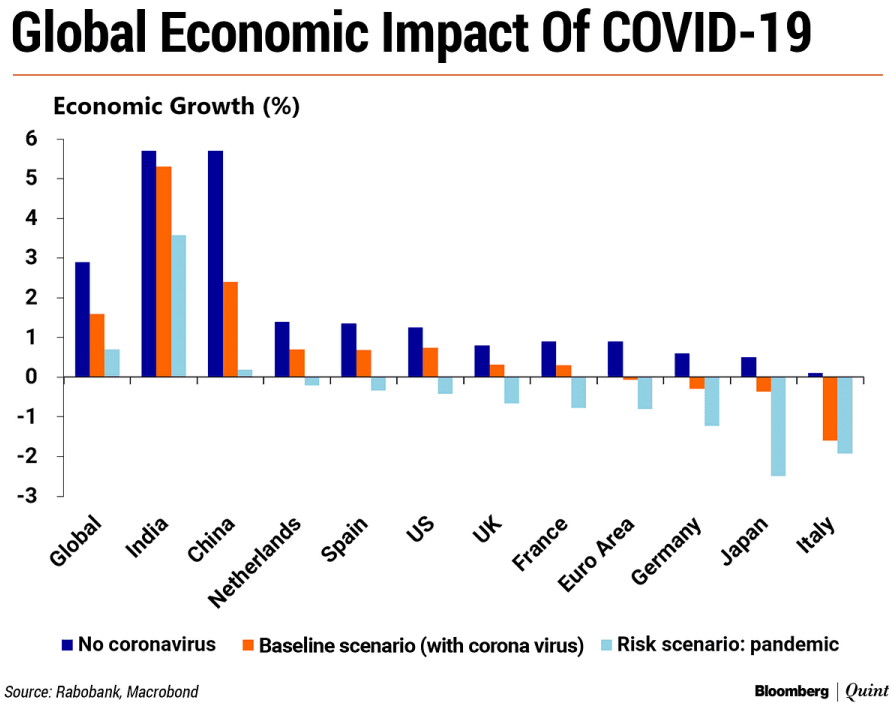
COVID 19 is disrupting the world in ways nobody ever predicted.

Currently, all major events in all top destinations are being counseled. There are doubts over the Tokyo Olympics. Football league games have been postponed.

All major industries are experiencing challenges - aviation, entertainment, education, and most critical the city life of big traffic- have been impacted. Economies that rely on tourism and aviation are feeling the pitch. Major tourism destinations are looking like ghost cities with hotels reporting just 10% occupancy, for the lucky ones. At one of the top hotels in Kampala, over 80% of the staff have been given leave for 30 days! It is unlikely that such leave is a paid one. The sudden loss of income is what will impact the global economy.

This COVID-19 virus is projected to cost the global economy more than two trillion US dollars (the US $2 Trillion). Now if this does not lead to a recession (two continuous quarters of negative growth), I don't know what else would lead to a recession in this century. Of most concern, the impact of things like these is not felt immediately. They are felt months and years later. That is the most worrying prospect.

To make matters worse, cybercriminals are preying on company emergencies and exploiting their digital resources. In graph 1, the global impact of COVID-19 is scaring. Without covid-19, the world economy was projected to grow at 2.9%. However, with covid-19, the growth reduces to 1.5%, or a worst-case scenario of the pandemic at 0.5%! The economy to be most hit are Italy, Japan, Germany, Euro Area, France, UK, US, and Spain in that order – as the worst-case scenario of a pandemic risks negative growth in these economies, which could lead to a prolonged recession.



Graph 1: impact of covid-19

Cybersecurity view

To the cybercriminals, the COVID-19 has provided an opportunity to undertake sophisticated social engineering

attacks by exploiting the confusion brought about by the pandemic.

When it comes to cybersecurity, we are seeing companies and health facilities being exposed because cybersecurity intelligence centers, people are no longer reporting to work. Yet cyber-intelligence, threat management, and cyber weaponry and cyber-warfare establishments involve lots of predictive analytics, and you need several eyeballs (people) to monitor trends and respond to any alerts in real-time. Much as machine learning and artificial intelligence capabilities can help, the human factor is still critical in case of emergencies due to the emerging nature of threats.

Due to security precautions, no company wants even their cyber-lab to be accessed remotely. People are not allowed in such centers to have unlimited remote accesses which makes off-site monitoring difficult. Companies that rely on outsourced services for cyber-intelligence are being affected. Also, employees are told not to come to work even if you do these services internally, the impact is huge. Now imagine a day away from the computer emergency response team! Companies must expedite remote working policy and set up capabilities to enable secure access for cybersecurity assurance.

How hackers are exploiting covid-19 to breach systems

Many hackers work alone at their laptop somewhere, under a command and control, in a distributed virtual network of professionals with a mission. They are always on the lookout of what is happening and lurking on networks that are not properly secured. Hackers are looking for zero-day exploits, poorly secured systems. Now if they find an organization that is not prepared or one which is prepared but without a team to identify the sources of threats and intrusions whatsoever on their networks, this means that they will have found a honey pot or 'gold' as a target for an exploit.

Enter social engineering

When it comes to cyber-breaches, social engineering is regarded as one of the oldest effective tricks but when coronavirus is in the play, it becomes even easier to track anxious users.

Everybody is afraid. Am I going to live past this pandemic? Pandemics have existed before but none has ever taken this trend like the COVID-19 and this has caused thirst for information to everyone. All links that would be a source of information seem attractive in the guise to offer know-how and know more about the pandemic and how to mitigate it. If you look at social media attacks like emails phishing luring attacks are increasingly happening.

People are interested in clicking to links that talk about the pandemic COVID-19 like "*How to protect yourself from COVID-19, proven ways by health specialists”*, *"Several deaths have been confirmed in a certain locality, see how it happened", “A president of the United States tested negative for COVID-19, his insights on how the pandemic is being worked upon.”*

Now, these and more have left everyone shaken up and ready to click to read more to find out how to safeguard against the virus as well as get updates about what is happening in the neighboring states. With a human curiosity to find out and clicking on links from email or social media, affects the way businesses are running. So, users need to be alert to avoid being victims.

The other attack vector to be aware of is a ransomware which is rampant where people offer a toolkit download for COVID-19 treatment and customize to your organization. It comes like a free toolkit with templates and notices to community COVID-19 awareness. Some HR staff is always interested in the solution and once they download it, it installs a rootkit that takes over the organization, depending on the security

posture and risk management maturity. We have responded to cases of ransomware.

In the absence of response and intelligence mechanisms, organizations and hospitals are currently being victims of these kinds of attacks. More so individuals on their digital assistants (PDAs) are being exploited and could feel the impact later when they report to work.

The main attack vector is phishing – sending a malicious link via email, mobile application, or social media enticing you to click it, which in the processes exposes you. As you read the article about COVID-19, in the background, spyware is being installed! In the absence of cyber-intelligence professionals and everyone not thinking in the line of security as a result of the natural disaster which destabilizes people's hope and at the end of the day the survivors will realize later that their intellectual property is recessively exposed.

Many downloaded files and apps on mobile files and computers are malicious and contain dangerous apps like rootkits, keyloggers among others that take over personal data.

Next steps

The government must have a coordinated response to protect both from the cyber and the physical point of view (should provide both health and digital readiness) regarding the pandemic. This is to provide a unified model of problem-solving where the government must put in place official sites regarding information repository for COVID-19.

The government should not only have a response on COVID management but also on cyber-readiness where the official digital resources for all information about the virus is available on a specified link.

For example, publishing on the specific mini-site on the Ministry of Health website as the official website for anything in regards to information about the virus and any links on this site are safe to be clicked and downloads safe for consumption by the mass. The government should source a

cyber response team that will give a security assurance of the content to be put on the site and to be downloaded to secure networks. This will help to provide a unified response strategy, providing security over the possible anticipated attacks with the overlaid attack vectors due to the occurrence of the pandemic and the fear of people that qualify them to be prey.

Such sites should be made secure and be kept up to date

Personal security

How to identify and protect yourself (as an Individual) from sites that harvest your information. Take note of the following to be secure.

When visiting a website that asks for sensitive information such as credit card numbers or your social security number, the first step you can take to securing your privacy is creating a strong password. Equally important is verifying that any information you enter on this site is transmitted and stored properly. Once your information is entered online, it is transmitted as plain text for anyone to intercept. To avoid this, make sure that the website is encrypted over a secure connection.

- HTTPS

One such sign to look for is in the URL of the website. A secure website's URL should begin with "https" rather than "HTTP". The "s" at the end of "HTTP" stands for secure and is using an SSL (Secure Sockets Layer) connection. Your information will be encrypted before being sent to a server.

- THE LOCK ICON

Another sign to look for is the "Lock" icon that is displayed somewhere in the window of your web browser. Different browsers may position the lock in different places, but a few examples of what it may look like can be found here:

Google Chrome

Clicking on the Lock icon will give you detailed information on the security status of this website

Mozilla Firefox

With Firefox, the Lock icon may not be displayed directly. Clicking on the site's icon next to the URL should reveal the Lock icon and the secure verification

Internet Explorer

Clicking on the Lock icon will give you detailed information on the security status of this website

Be sure to click on the "lock" icon to verify that a website is trustworthy. Do not simply look for the icon and assume a website is secure! Your web browser will have detailed information on the website's authenticity if you click on the icon, so be sure to read this carefully before entering any of your information on the site.

Other ways to safeguard against website schemes are;

- Read the URL carefully. If you frequently visit this website, check if the URL is spelled correctly. Often, phishers will set up websites almost identical to the

spelling of the site you are trying to visit. An accidental mistype may lead you to a fraudulent version of the site.

- Check the properties of any links. Right-clicking a hyperlink and selecting "Properties" will reveal the true destination of the link. Does it look different from what it claimed to lead you to?

Be secure.