# **CYBER ATTACKS DURING COVID19 AND PRECAUTIONS TO BE TAKEN**



2:16 PM (2 hours

## **PHISHING ATTACKS**

Emails are sent to very large numbers of recipients and groups, and typically is random , luring the receiver into revealing sensitive information through mails

#### EXAMPLE:

Mail Stating; "The world has never faced a pandemic like COVID19.Click here to support Migrant workers, Sanitary Workers in BTC. Let's stand together". Solidarity Response Fund. Help WHO fight COVID-19 D Spam ×

8	This message seems dangerous Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

The world has never faced a crisis like COVID-19. The pandemic is impacting communities everywhere. It's never been more urgent to support the global response. The humanity, solidarity and generosity of people and organizations everywhere is also unprecedented. But we can't stop now.

The World Health Organization (WHO) is leading and coordinating the global effort with a range of partners, supporting countries to prevent, detect, and respond to the pandemic. Donations support WHO's work, including with partners, to track and understand the spread of the virus; to ensure patients get the care they need and frontline workers get essential supplies and information; and to accelerate research and development of a vaccine and treatments for all who need them.

See below for more ways to give, Via BTC (Bitcoin). Every donation helps support lifesaving work for the world.

### PRECAUTIONS

- 1. Examine the sender's email address to **ensure if it is from a true account**. Hover over the link to expose the associated web addresses in the "to" and "from" fields;
- 2. Note grammatical errors in the text of the email; they are usually a sure sign of fraud.



New notification ,Please due to COVID-19, all staff & Employee are expected to kindly Click PROCEED and complete the required directive to be added to March and April benefit payroll directory as compilation is ongoing and will last within 48hours.

Thank you, Admin Department

## SPEAR- PHISHING ATTACKS

Carefully crafted fake email targeted to an individual mails in an attempt to obtain sensitive information like passwords, account details or expecting monetary favoursand are very common in enterprise scenarios.

#### EXAMPLE

#### Mails stating,

"Dear Staff, The employees are requested to click the link to complete the directive within 36 hours for adding into March-April payroll directory".

## PRECAUTIONS

- 1. Examine the sender's email.
- 2. **Report suspicious emails** to the IT / Security department of the Organization.
- 3. Don't forward suspicious emails to co-workers

## MALWARE ATTACKS

Asks the user to download attachments claiming to be official notifications released by WHO and other known Organization.

#### EXAMPLE

 Email impersonating WHO that claims to have documents attached that includes latest news on COVID19 vaccine release. The attachment may be a rar archive, doc, pdf that includes .exe file which is a Nanocore RAT malware.

## PRECAUTIONS

- 1. Be skeptical of pop-ups, emails from unknown senders.
- 2. **Don't click** on links or open attachments from those senders.
- 3. Use updated version of Antivirus



From:	COVID-19 Relef - Sarin Danink LICTTO (gara saring	Sent	Wed 3/18/2020 ii
Tol	+1928-L1+24		
Cc			
Subject:	COVID-19 Payment		
Hessage	COVID 19 Relief.doc		
Canadian Here is th	Prime minister Justin Trudeau approved an immediate check of \$2,500.00 -/CAD for those who choose to stay at home during e form for the request. Please fill it out and submit it no later than 25/03/2020.	the Core	onavirus crisis.

## RANSOMWARE **ATTACKS**

Asks the users to enable view the macros to downloaded attachments. Once enabled, encrypts the file system entire and demands the user to pay in BTC to decrypt the files.

#### **EXAMPLE**

• Zeus Sphinx that surfaced three years ago is attempting again through mails claiming to offer financial relief.



## PRECAUTIONS

- 1. **Disable Macros** while using Microsoft Office.
- 2. Maintain Periodic Back-ups.

## TARGETED ATTACKS

Threat actors focus only on specific compromising а entity over a period of time.

#### **EXAMPLE**

- Hackers have forced the Italian social security website to shut down for a period.
- Maze Ransomware has disruption caused to services and systems at Cognizant.

## PRECAUTIONS

- 1. Secure your Wi-Fi access point. Change default settings and default passwords in order to secure your home network.
- 2. Avoid accessing the socialnetworks like Facebook, Twitter etc., from the system that you access the office network.
- 3. Do not connect to public/open Wi-Fi networks. Use a separate home internet network for work to isolate personal devices.
- 4.'Remember password' function should always be turned off when you are logging intoyour organization'ssystems from your personal devices.
- 5. Strengthen your remote access management policy and procedures. Implement multifactor authentication for VPN access, IP address white listing, limits on remotedesktop protocol (RDP) access.

### Forwarded

RASAM - Antidote For Wuhan Virus By Manidar Nadeson, holistic healer

### **FAKE NEWS**

Fake news, video clips, GIFs, authentic-IOOKING federal government connected to coronavirus (COVID-19) has been making rounds in the internet.

Many years ago when Malaysia was hit by the Nipah virus, malaysians indians was not affecrted the reason most of them consumed RASAM a tamilan soup that is made from mix of herbs. If rasam is with a mild temperature the body will react to heal any kind of viruses. It is encourage to drink with some hot rice for better effects. It was put to trial during the SARS epidemic and the results are amazing. Preventive is better than cure start today for tomorrow, the Rasam". Avoid consuming meat that is not properly cooked. Rasam" the best way forward to 5:47 AM

cure Wuhan viruses.

PRECAUTIONS

#### **EXAMPLE**

#### Messages stating,

- "Vaccine for COVID19 found and can be made at home".
- Fake Messages making rounds on the internet stating, "Rs.5000 will be credited as part of COVID Relief Measures"

1. Do not forward messages without verifying the credibility and authenticity of the message

## VIDEO-BOMBING

People unrelated to the user groups are found to be appearing/joining the calls made via video conferencing app

#### **EXAMPLE**

 Zoom-bombing conference calls has become more common.

## PRECAUTIONS



1. Using alternative audio and video conferencing environments like Microsoft Teams, Google Meet and Rocketchat and open source alternatives include Jitsi for communication with colleagues.



## DENIAL-OF-SERVICE AND DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

Attackers/Group of attackers make subsequent request to servers preventing the legitimate users from availingthe service

#### EXAMPLE

• Video-Conferencing apps have been targeted in the recent times.

### PRECAUTIONS

1. **Monitoring the traffic** that ingress the server and employing end-point security devices.

## **CROSS-SITE SCRIPTING ATTACKS**

The attacker could send the victim a misleading email with a link containing malicious JavaScript. If the victim clicks on the link, the HTTP request is initiated from the victim's browser and sent to the vulnerable web application. The malicious JavaScript is then reflected back to the victim's browser, where it is executed in the context of the victim user's session.

#### EXAMPLE

#### Mail Stating;

"Pay just Re.1 to contribute to COVID Relief fund by clicking on the link".Clicking the link takes the user to the user's net banking site asking the user to input passwords.The attacker could steal the passwords of the victim when the victim click on link.

## PRECAUTIONS

1. **Ensure the authenticity** of the links and do not pay to charity from unknown charity fund collectors.





## **DRIVE-BY ATTACKS**

When a visitor navigates to a site that injects malware onto the victim's PC, runs in the background invisible to the user without the user taking any



## PRECAUTIONS

1. Do not visit HTTP sites .

conscious action steps to initiate the attack.

#### EXAMPLE

- Domain names of sites crafted to appear like the authentic websites might contain drive by downloads
- http://covidmedicine.amazon.in
- 2. **Update systems and software**. Install updates and patches in a timely manner, on mobile devices and other non-corporate devices you might use for work.
- 3. **Do not leave your systems unattended** at home. Creating a separate user for your system might be helpful if your laptop is going to be used by other members of the family.
- 4. Install Organization-approved Anti-phishing filters on browsers, USB media devices and to scan attachments. Indigenous tools like USB-Pratirodh, AppSamvid, JS Guard by C-DAC come in handy

# **References:**

- 1.https://infosecawareness.in/article/covid19-cyber-attacks
- 2. https://cloud.google.com/blog/products/identity-security/protecting-againstcyber-threats-during-covid-19-and-beyond
- 3. https://www.securitymagazine.com/articles/92157-coronavirus-related-spearphishing-attacks-see-667-increase-in-march-2020
- 4. https://www.forbes.com/sites/leemathews/2020/03/31/criminals-resurrect-abanking-trojan-to-push-covid-19-relief-payment-scam/
- 5.https://twitter.com/MBThreatIntel/status/1247669823405830144