COVID-19 THEMED MALICIOUS CYBER ACTIVITIES

-THREAT UPDATE v1.0

Published on: 07.04.2020

Dr. Maithili Sharan Gupta
Director General of Police (Police Reforms)
Madhya Pradesh Police Department

Dr. Shishir Kumar Shandilya
Division Head, Cyber Security & Digital Forensics,
Vellore Institute of Technology, VIT Bhopal University

Student Editorial Board*
Mr. Saket Updhayay, Software Security
Mr. Fardeen Ahmed, Web Security
Mr. Divyansh Bhatia, Technical Content Creation
Mr. Sanchit Bajaj, Graphic Design

**Students of II year BTech (CSE: Cyber Security & Digital Forensics), VIT Bhopal University*

VIT BHOPAL

OVERVIEW

This threat update is intended to make the netizens aware about the on-going malicious activities by using the term COVID-19. These specially crafted activities and attacks are attempting to make use of panic and discomfort caused by COVID-19 pandemic for their own malicious-interest. This document will provide information on how to mitigate these attacks and reduce the risk of being impacted.

The spread of a dangerous novel coronavirus COVID-19 is on the rise. While the nation is fighting the disease in the real world, cybercriminals have caused havoc in the digital world by targeting the innocent victims in this difficult time.

The spread of the novel coronavirus gives cyber-criminals a perfect opportunity for scaring people or scamming them for money or resources. These practices include setting up legitimate-looking websites to impersonate official websites and spreading false information online. It is important to take precautions, both physically and digitally.

With very little efforts, these attacks can be modified with a COVID-19 theme which makes them much more dangerous. At a time, when people are physically vulnerable, managing cybersecurity is difficult. It is also possible that these malicious actors are operating from outside the country, which makes it much more difficult to apprehend them in case of any loss.

Apart from applying the technological tactics, they are also exploiting the emotional state of the people. Messages such as *"Get 25 GB of data free by upgrading your application"* and *"Get extra money while working from home"* are exploiting the needs of people during the lockdown period.

It is strongly advised that while working online, the netizens should stay vigilant.

CURRENT CYBER ATTACK TRENDS

Utilizing the panic created by the coronavirus outbreak across the globe, the attackers are targeting a wide range of establishments from individual users to corporate organizations and government assets. It is important for everyone to stay informed and careful against such attacks by these cyber adversaries.

As almost everyone is working from home, it has impacted the quick development of Cyber Security solutions. Due to this slow down, patching software vulnerabilities will take longer time than usual. Internet users are adviced to remain extra vigilant when dealing with outdated software.

During the lockdown, with work-from-home being implemented in many organizations, people's interaction with digital devices and the Internet is far more than ever, and this provides an excellent opportunity for attackers to get potential targets. Malicious actors are launching various attack campaigns, scams and phishing campaigns against the general public who are soft targets to them due lack of awareness of these kinds of attacks.

CASE #1: AZORULT TROJAN

This four-year old malware strain has reappeared with a new design to fit in the COVID 19 theme. It has been traced back to some malicious applications which are intended to steal data from target devices including sensitive login credentials and banking details.

The malware attempts to target with a malicious email that claims to be from the Government or WHO (World Health Organization) and having some attached files titled as "cures for coronavirus." Once the file has been opened, the malware gets executed in the target system.

From : ctnprincipal@inscape.co.za Date Time : 9/4/2019 10:05:07 PM
To : [redacted]
Cc :
Bcc :
Subject : Re: As Agreed
Attachments : attachedFile.rtf Attachment_74754756754675467509097823632734563434.img

[EXTERNAL EMAIL] Verify sender before clicking on links or attachments

Good day,

Kindly find the below documents as you requested, Please Sign on the last 3 pages where your initials and Banking informations are then we can proceed with payment.

Your soonest response will be highly appreciated.

Best Regards
Njisuh Zebedee
Assistant Manager
1 Forssman Close, Barbeque Downs 16185
Fax: 0822748278

CASE #2: SPOOFING

Attackers are also targeting government schemes such as the **PMCARES** fund by using similar-looking UPI IDs, spoofing official websites, and spreading fake news. Moreover, they are also sending confirmation e-mail/sms for the successful transfer of funds. Many people are unable to identify it, as it is a normal bank transaction. The only difference is the destination of fund transfer.

SBI

BE KIND, BE WISE

In these tough times, many fraudsters are scamming people in the most devious ways.

LOOK WHERE YOU DONATE!

pmcarefund@sbi
pm.care@sbi
pmcare@sbi
pncare@sbi
pncares@sbi
pmcaree@sbi
pmcaress@sbi

pmcares@sbi

PMCARES

pmcares@sbi
Scan & Pay with BHIM UPI app

BHIM UPI

SBI Advisory

भारतीय आयुर्विज्ञान परिषद्
MEDICAL COUNCIL OF INDIA

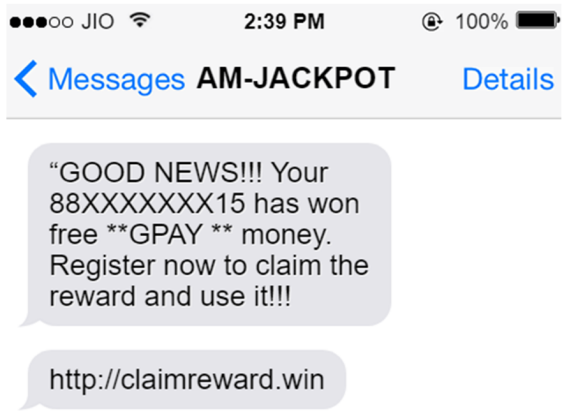
FAKE
FAKE
FAKE

Example of fake/forged official document

CASE #3: BANKING PHISHING

Messages such as *"Get 2000 in your PAYTM wallet"* or *"Free GPAY money"* are in circulation. Cyber-criminals are using these messages to extract bank account details from the target user. The criminals are after debit/credit card details used to access UPI accounts.

It's requested that you don't respond to these messages at all and report them to the police at cybercrime.gov.in



Phishing SMS Example

A quick advice to avoid this:

- Read the message very carefully.
- Never act immediately on the advice given in the message.
- Never open any link (URL) if the message seems suspicious.
- Mark the message as spam once it is identified so.

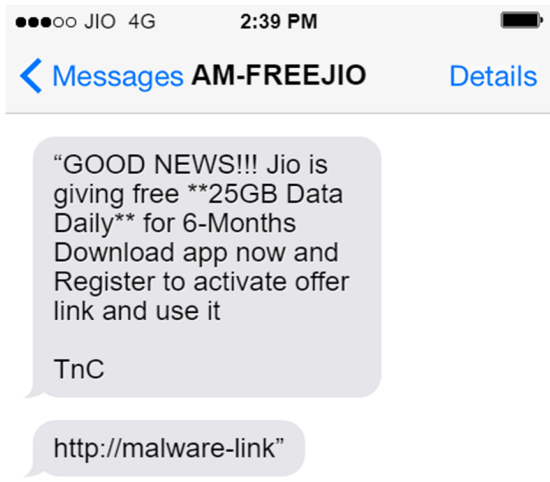
Don't share any banking details with anyone, despite how important they may make it seem.

CASE #4: JIO MEMBERSHIP WORM

Onboarding Screen

This trojan was distributed to citizens of India as SMS with the link to a safe-looking web page which asks the target user to download an application and install it on their mobile phones. After installation, the application creates a backdoor and sends a spam SMS to all the contacts impersonating the user. The target user becomes the culprit.

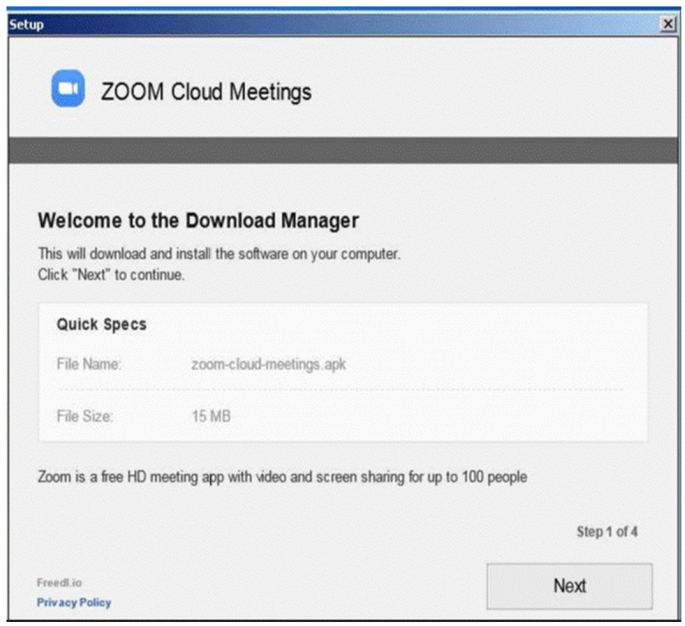
Here's what the text message looks like-



CASE #5: ATTACKS ON OUTDATED SOFTWARE AND INFRASTRUCTURE

With the rise of pandemic stress and surrounding tension, attackers are targeting outdated software and infrastructure with known/unknown vulnerabilities as they are not being maintained or patched regularly. Work-from-Home platforms are also under attack as corporations and businesses depend on them. They do this by sending malicious links to employees or by exploiting vulnerabilities in these platforms.

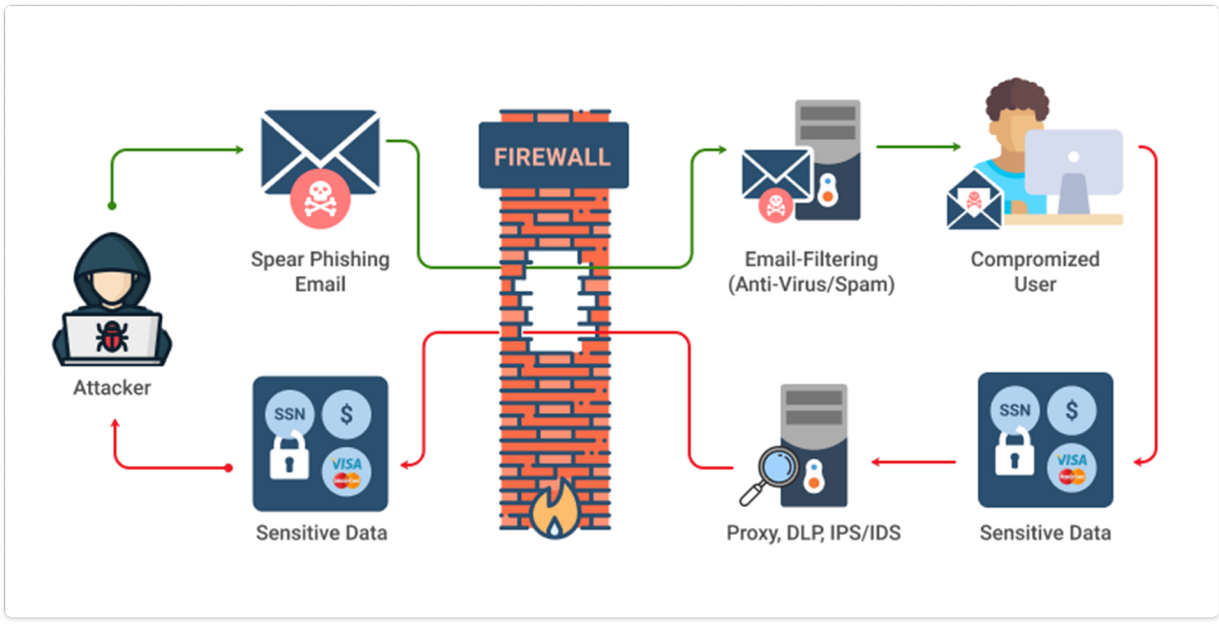
Popular meeting platforms are the major targets. Hackers are replacing the original installer program with malware-embedded software for windows.



A Zoom flaw gives Hackers easy access to your Webcam

CASE #6: SPEAR PHISHING

Malicious actors are performing targeted attacks on the client base, spoofing and phishing company assets, and clients. Attackers are targeting clients and employees to steal personally identifiable information with an intention to steal banking information or to gain influence in the target company.



Process of Spear Phishing

MITIGATION TECHNIQUES

While these attacks are in progress, it's important that everyone stays safe digitally. In order to save citizens from these types of attacks and prevent major digital crisis, here are few practices that one should follow:

FIGHT AGAINST FAKE NEWS

Fake news on social media spreads faster than wildfire. The proliferation of fake news about the COVID-19 pandemic has been labelled as a dangerous "Infodemic". While the government and platform owners are fighting the spread of fake information on the larger level, being a responsible citizen, you can also help at your level. Here are some guidelines to help avoid the spread of fake information online:

• **Stop forwarding the chain messages:** Whenever you get a message that is in relation to some important news on COVID-19, before forwarding, please confirm it. Use three to four trusted news media sources to collaborate and confirm the news first.

• **Identify fake news:** To catch the attention of people, fake news sources add a few characteristics to their message. Some messages also have faults that are starkly visible. These include, but are not limited to:

Use of poor language: The fake news sources usually have poor language construction or lack professionally themed language. Please note that any official news source takes serious precautions with language so as not to promote the wrong idea. But, for someone who is jotting down the fake news, how people interpret it is of no concern.

Use of emojis or stickers: Emojis are used to make a written piece eye-catching. But, watch out for the use of too many of these emotional portrayals. No message from any news source will contain an emoji, no matter how frank it is with its audience.

Forwarded by too many people: Some social media sites allow you to see that how many people have forwarded a message or how many people have been tagged into the message. News media sources understand search engine optimization and will tag no more than five well-known sources. If a message has too many sources tagged, take it with a grain of salt.

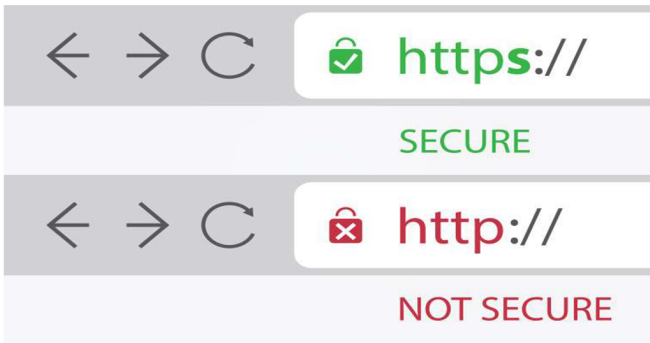
• **Fight the message:** There is always a comments section on a message, or you can always reply to a message. What to comment on? Using your research, comment on how or why the information is wrong. Quote official news sources if necessary.

• **Forward the actual news:** Instead of forwarding the fake news, forward the official news source along with the actual news.

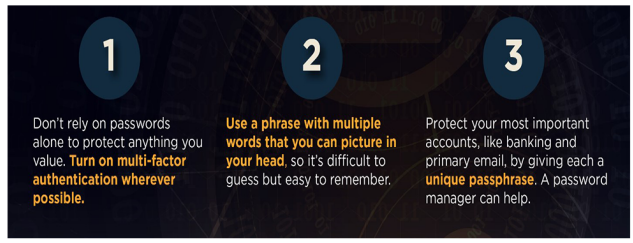
It is a legal offence to try and communalise the public using the issue of coronavirus. Offenders can be booked under section 153A and many other sections of the Indian Penal Code for spreading such false information online.

SAFE WORK-FROM-HOME PRACTICES

- Practice **Zero Trust Policy** i.e. don't trust anyone digitally, and always crosscheck everything online.
- Do not click on suspicious links received via email or SMS.
- In case of doubt, copy the link and do a google search, maybe someone else with the same experience might have posted something on the internet.
- Try not to download/install unknown/unnecessary applications on your smartphones.
- Do not trust or spread any news from untrusted or unverified sources.
- Keep your PC updated with the latest software.
- Update video conferencing software to their latest versions.
- Use strong passwords, must be at least 12 characters long with a combination of uppercase (A-Z), lowercase (a-z) letters, numeric characters (0-9) and special characters (,._/?;@#&*!$)
- Update WiFi, social or professional account passwords regularly.
- Do not share your Zoom, Microsoft Teams, Skype or other meeting IDs in social media posts. Hackers are always there for our small mistakes.



HTTPS websites are more secure



Strong Passwords keep you safe

SAFE EMAIL PRACTICES

Malicious emails may appear as the following:

- Emails impersonating W.H.O. (World Health Organization), contacting about "Cures of Coronavirus".
- Phishing Emails asking you to make important transactions because banks are going to close soon.
- A reputed medical professional mailing you about a Secret/Homemade Cure for COVID 19 disease.
- An Email with one attached excel sheet containing latest infomration about the infected people in your area.

You can use the following tactics to protect yourself from these attacks:

- ✓ Check for the actual source of the email.
- ✓ Check for the tone of language and its format, don't respond to unknown people or suspicious email.
- ⊘ Do not visit/click unknown or suspicious links.
- ✓ Check the actual embedded link by hovering the mouse cursor over it.
- ✓ Try to visit the links manually, by typing it in the URL box of your web browser.
- ✓ Check for a green lock and "https://" in the URL bar.

WHERE TO REPORT?

If you think that you have been a victim of a cybercrime, dont fret. Report it immediately to **cybercrime.gov.in** or give a call at **155260**. If and only if, you think it is safe to go outside, then you can also report it to the nearest cyber cell. However, the second alternative is recommended only when the issue is critical, with prior consultation with the police over phone. To stay connected with doctors 24x7 and to get updates on COVID 19 in your area you can use the **Aarogya Setu** app from https://www.mygov.in/aarogya-setu-app.

The only one you can trust is you, and be prepared always.

To be safe, report any crime at the earliest possible.

Sources:

1. https://www.webarxsecurity.com/covid-19-cyber-attacks/
2. https://www.varonis.com/blog/covid-19-threat-update-3/
3. https://economictimes.indiatimes.com/tech/internet/cy4. ber-chiefs-warning-as-hackers-target-pms- covid-fund/articleshow/74877953
4. https://www.csoonline.com/article/3532825/6-ways-attackrs-are-exploiting-the-covid-19-crisis
5. https://m.economictimes.com/tech/internet/hackers-are-usg-covid-19-disruption-to-infiltrate-corporate-networks/articleshow/74837213.cms

Further Readings:

1. www.who.int/about/communications/cyber-security
2. www.hindustantimes.com/tech/hackers-are-prey ng-on-fears-of-covid-19-says-cyber-security experts/story-4SIki55hdtVLRycZgjz7JO.html
3. https://economictimes.indiatimes.com/wealth/save/coronavirus-online-scams-how-to-protect-your-data-and-device/articleshow/74862378.cms?from=mdr
4. https://success.trendmicro.com/solution/000146108-AZORULT-Malware-Information
5. https://www.zscaler.com/blogs/research/covidlock-android-ranomware-walkthrough-and-unlock
6. https://cybercrime.gov.in

VIT®
BHOPAL