



Cyber Threat Report

COVID-19

 **K7 SECURITY**

www.k7computing.com



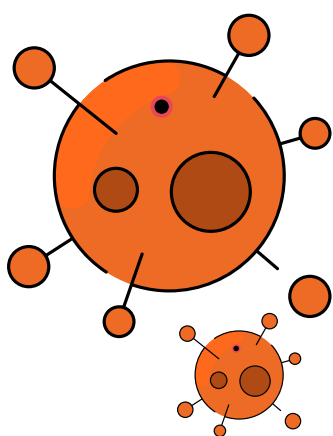
Cyber Threat Report Covid-19

Table of contents

Attack Trends Amid the Coronavirus Pandemic	3
Trending: Covid-19 Related Attacks Across India	5
Rising Number of Corona Theme Based Phishing Attacks	7
Google on Covid-19 Themed Malware Attacks	8
Safety Precautions	9
Corona Theme Attacks on Mobile Devices	10
In India	11
Coronavirus Themed App Promises Safety Masks	11
Across the Globe	12
Project Spy - A Spyware campaign	12
Banking Trojans Profiting from Corona Based Campaigns	13
Ginp & Anubis	13
Case Study: Cerberus Trojan Targets Mobile Devices	14
Tips to Stay Safe	15
Attacks to Continue	16

Attack Trends

Amid the Coronavirus Pandemic



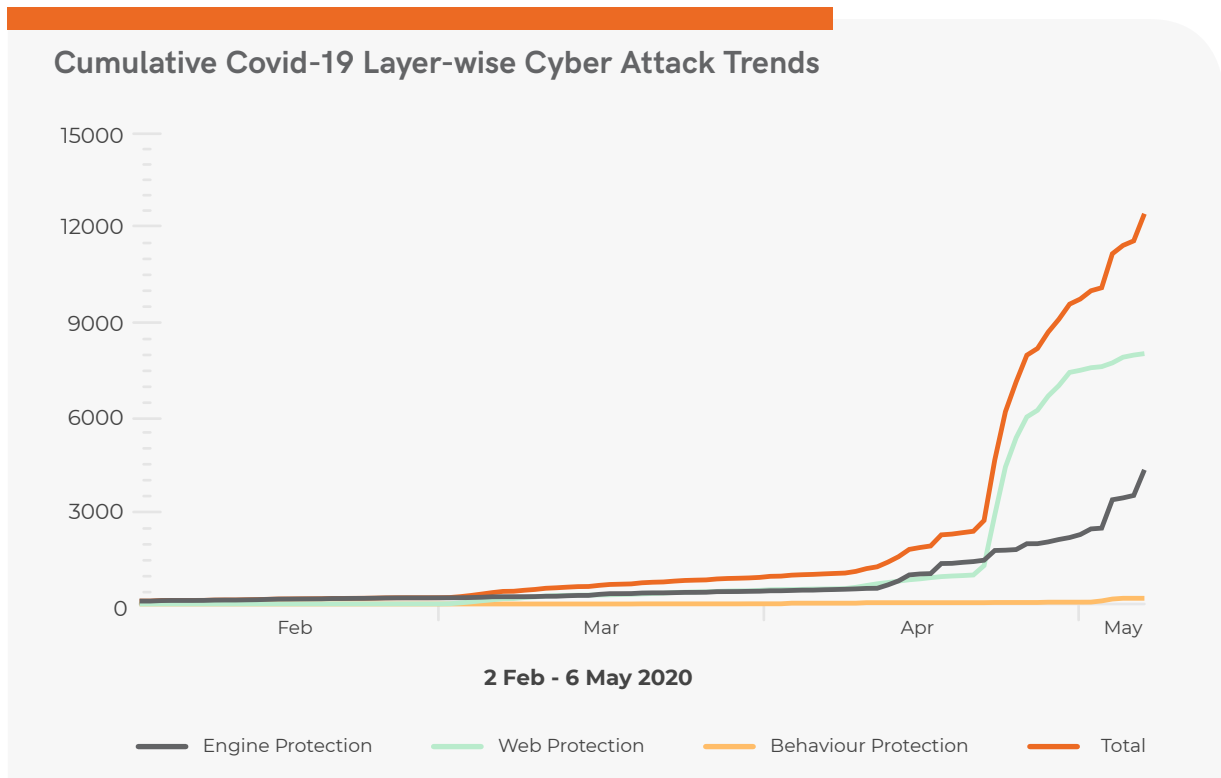
Scammers across the world are actively manipulating the widespread panic about the Coronavirus outbreak after it was announced as a pandemic by the World Health Organisation (WHO). Using this global scare as the theme of their attack, cybercriminals are coming up with different methods to deceive users across device platforms.

Over the past couple of months, we have noticed an increase in the number of phishing attacks. Threat actors are actively executing massive phishing campaigns against large enterprises, SMEs, SOHOs and end-users under the disguise of legitimate organisations such as the World Health Organisation (WHO), U.S. Ministry of Health and many others. Alongside, we also noticed a growing trend of ransomware-based targeted attacks prevalently eyeing the healthcare industries, which include the Covid-19 major testing hubs and hospitals. The ramifications of such attacks during the coronavirus outbreak could be devastating to the society at large.

We at K7 Labs, on analysing stats obtained from our telemetry data, observed that starting from February to mid-April 2020, an upswing was observed in Covid-19 related website visits in the Tier-1 and Tier-2 cities of India. During this period, the K7 Web Categorisation engine had processed almost 178000 URLs visited by K7 Security users which are all Covid-19 related, of which about 1700 unique domain names explicitly refer to the Covid-19 pandemic. Most of these URLs are, in fact, legitimate and are supposed to be informative. Yet, the volume of Covid-related traffic and its popularity demonstrates how easy it would be for cybercriminals to get victims to visit fake Covid sites during this period of stress and fear that is spreading across the globe.

Of the URLs mentioned, more than 60 are confirmed malicious whereas a few others which were malicious earlier have been taken down at the time of writing.

We also looked carefully at our backend telemetry data within K7 Ecosystem Threat Intelligence (K7ETI) over the 3-month period from the beginning of February to the beginning of May 2020.



Looking at the upward trend in the chart mentioned above clearly demonstrates an abundance of Covid-19 based threats that were blocked at three of our core threat protection layers. The frequency took a significant upswing, especially after the end of February 2020 when people around the country started to become more anxious and desperate for legitimate information about this pandemic, and a spike is clearly visible after the first phase of the Lockdown was announced.

Covid-19 themed cyber threats in India were found aplenty which is in addition to the regular frequency of cyberattacks that are encountered on a daily basis.

Trending: Covid-19 Related Attacks Across India

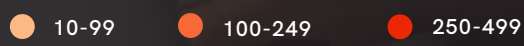
One measure of the frequency of attacks that have been encountered may be calculated as the number of Covid-19-related attacks that were blocked per 10000 active and unique users reported to K7ETI in the corresponding geolocation.

Starting from February 2020, we noticed a number of Coronavirus online scams mushrooming in the Tier-2 and Tier-3 cities across the country. The recorded number of users who encountered such threats during the period remained noticeable in cities like Kottayam, Kannur, Kollam and Kochi. However, users in the Metros appear not to have encountered these scams, possibly due to them following better cybersecurity hygiene practices.



It is surprising to see from our stats that many Tier-2 and Tier-3 cities had faced the major brunt of Covid-19 themed attacks. For instance, Kottayam, Kannur and Kollam were affected the most. More than 250 attacks were blocked per 10000 active users in these cities respectively. Users from Ghaziabad and Lucknow seem to have faced almost 6 and 4 times the number of attacks as Bengaluru users. Similarly, other cities like Patiala, Thiruvananthapuram and Hoshiarpur have also experienced a relatively higher number of attacks compared to the big metro cities like Mumbai, Delhi or Kolkata at the time of writing.

Covid-19 Related Attacks Across India



Number of attacks blocked per 10000 users

Map for illustrative purposes only. Not to scale.

Rising Number of Corona Theme Based Phishing Attacks

Phishing attacks in the country are continuing to increase, further supporting the notion that adversaries are embracing new tools and techniques to capitalise on human error. During this coronavirus outbreak, K7 Labs observed that phishing campaigns have outnumbered other Covid-19 themed attack methods. Threat actors are using several sophisticated campaigns as bait to trap unsuspecting victims.

Modern threat actors are more knowledgeable and dexterous than their predecessors. Even the most educated users could be deceived into clicking malicious links and revealing their sensitive information or downloading malware onto their devices, without even an iota of hesitation. For instance, we noticed a phishing attack where the scammers in the guise of a United States Department of Treasury representative falsely assures victims to activate their deactivated ATM cards in exchange for an up-front payment.

By impersonating legitimate and reputed organisations like The World Health Organization (WHO) and The Centers for Disease Control and Prevention (CDC), bad actors are executing targeted phishing campaigns for delivering malicious payloads. Some of these campaigns have even dropped dangerous malware onto the victims' devices such as the Agent Tesla keylogger or Lokibot information-stealing malware, infamous banking Trojans such as Trickbot or Zeus Sphinx, and even disastrous ransomware.

The targets of such campaigns are primarily healthcare, research and government industries.

We have also found many instances where malicious Android apps claiming to be legitimate coronavirus tracking apps dropped ransomware on the user's device and demanded payment to restore access to the device.



Google on Covid-19

Themed Malware Attacks

In April 2020, the popular search engine giant "Google" reported that it had blocked around 18 million Covid-19 themed malware and phishing campaigns daily. Alongside, it was also filtering out roughly 240 million Covid-19 themed spam messages every day.

The success of these attack methods is because scamsters create a sense of urgency by igniting the victim's fear of the pandemic, and also by luring them with monetary benefits. Many victims usually respond to this trap laid by the threat actors who then steal sensitive information or drop dangerous malware onto the victims' devices.

Google also added that there were only minor tweaks to the message subject line and the email body content, while the scams were all essentially the same; impersonating reputed organisations like The World Health Organization (WHO) and The Centers for Disease Control and Prevention (CDC).

Apart from these scam emails, bad actors were also increasingly targeting employees working from home. We found many such spam emails sent to large enterprise and SME employees impersonating a higher authority from the same company.

The situation is worse for organisations who have hurriedly adopted remote working policies considering the safety of their employees and the organisation, without having any strict cybersecurity guidelines for working remotely. Organisations are advised to ensure their employees follow best cybersecurity practices while they allow them to work from home.

☰ Email

🔍 Search mail



Inbox
Starred
Snoozed
Sent
Drafts
Chats
Spam

WHO Corona funds Inbox X

John doe <johndoe@gmail.com>
to me

Safety Precautions

- Do not open emails from unknown sources
- Check the senders' email ID to confirm if it is from the said originator
- Check for unwanted characters in the email content, and check if the email is addressed specifically to you
- Do not get carried away by hackers who increase the priority of emails with capitalised keywords such as URGENT/ATTENTION/TOP PRIORITY, in the subject/body and highlighted content in the body of the email
- Check for hyperlinked text; do not click on it but instead, carefully see if it is a legitimate one by only hovering your cursor over the link
- Check for sentence phrasing and grammatical mistakes
- Check if the attachments are appropriately named and safe
- Check for the credibility of the undersigned, e.g. check for the sender's name in the email signature
- Do not enable macros by default for Microsoft Office documents. The result could be the dropping or downloading of malware
- Check for the legitimacy of the URL before revealing confidential information
- Ensure the OS and all applications are updated and patched for the latest vulnerabilities
- Keep your security product updated and use a reputable AV product like K7 Total Security
- Scan your devices regularly

Corona Theme

Attacks on Mobile Devices

Threat actors are leaving no stone unturned to lure target victims, and in the process, they have also started to increasingly focus on the smartphone app market; deceiving users with malicious apps. Though most of the apps don't make it to the official app stores, the bad actors promote them enough via impersonating legitimate sites, shady app stores and using black hat Search Engine Optimisation skills.

In the past couple of months, many Covid-19 themed malicious apps have been doing the rounds, tricking users into installing them onto their devices. Let's get into the nuances of a few such apps.



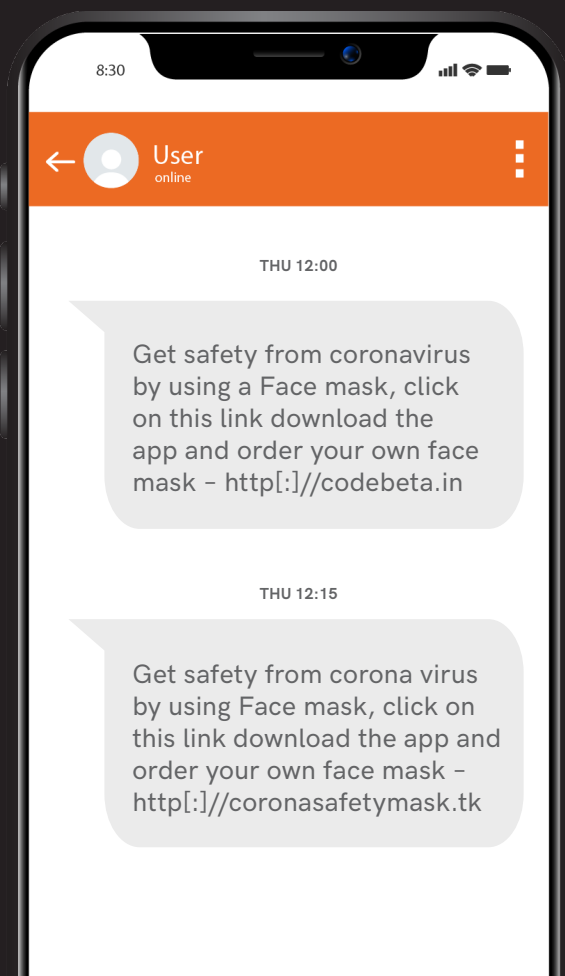
In India

Coronavirus Themed App Promises Safety Masks

Recently, Android devices were scammed by an SMS Trojan. The Trojan spreads via SMS that directs the user to install an app named "CoronaSafetyMask" to receive Safety Masks.



THE SMS READS:



Once the victim installs this app, it requests permissions to read the victim's contacts and send SMS. It then directs the victim to click a button that leads to an online portal which supposedly sells masks online. The app then checks whether it has already sent the above SMS messages or not to all the contacts in the victim's contact list. If it has not, it sends either of the above text messages to all the contacts, to trick other victims into installing the app, resulting in a significant amount of potential SMS charge for the sender.

Across the Globe



Project Spy - A Spyware campaign

An app dubbed Corona_Virus.apk, promoting itself as the deliverer of information updates about the Coronavirus pandemic, is doing the rounds via phishing links and has been targeting Android. A similar campaign exists for iOS devices too. This campaign is named "Project Spy" based on the login page of its backend server. Once installed, the "Coronavirus Updates" app gains the capabilities to:



- Upload WhatsApp, Telegram, Facebook, GSM and Threema messages
- Upload contacts, call logs, location information, voice messages
- Upload device and SIM information

It is, however, not an exhaustive list of this spyware's capabilities.

Banking Trojans Profiting from Corona Based Campaigns

Banking Trojans such as Ginp, Anubis and Cerberus are taking advantage of the growing fear about the pandemic among people to spread malware.

Ginp & Anubis

While the Ginp Trojan disguises itself as the app "CoronaFinder" and promises to provide the location information of coronavirus-infected people around the user on the payment of a small amount, it instead opens a webpage called coronavirus finder and asks the user to input data to make the transaction. However, once the user enters the card details, it steals this financially-sensitive information. The Anubis Trojan masquerades itself as a coronavirus statistics app in the name of covidMappia_v1.0.3.apk and hides itself to steal the user's sensitive information.



Case Study: Cerberus Trojan Targets Mobile Devices

This Banking Trojan disguises itself as a benign Covid-19 app, covid-19.apk, which is capable of stealing credentials and sensitive user data. This malware has targeted more than 250 banking and cryptocurrency applications across the globe. Some of the Indian banks that have been targeted by this malware are Axis bank, ICICI Bank, Indian Bank, and HDFC Bank to name a few.



Operation Cerberus



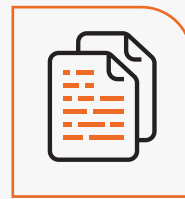
UNDER THE RADAR

Masquerades itself as a Flash Player App to stay under the radar



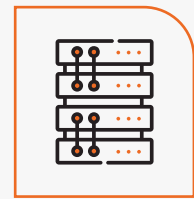
THE CLINCH

Gains controls of the accessibility service of the device to monitor user's activities



THE DUPE

Launches a fake overlay login page whenever the user intends to login to any targeted banking service



LINKBACK

Sends the collected financial credentials to the C2 server

Once this app is installed on the device, it first ensures that it gains control of the accessibility service of the device to monitor the user's activities stealthily. It also masquerades itself as a genuine Flash Player Application and hides its icon to stay unnoticed. Whenever the victim opens any banking app, the Trojan opens a fake overlay screen, a phishing login page of that targeted application, where it asks the user to enter their confidential information. This malicious app also has Remote Access Trojan (RAT) and keylogger functionalities which steal confidential information when the user inputs account credentials by logging keystrokes, recording sound and saving the log file to send to the Command & Control (C2) server. It also disables "Google Play Protect" to prevent its discovery and removal.


Tips to Stay Safe



- Install apps only from the Google Play Store
- Avoid clicking on unknown links delivered via SMS, emails, etc.
- Always disable "Install unknown apps" on your Android devices
- Keep your security product up-to-date and scan all your apps with a reputable security product such as "K7 Mobile Security"



Attacks to Continue.....



The prevalent number of Covid themed attacks will continue to increase, at least till the crisis begins to subside and may continue to persist; especially those that use social engineering techniques which manipulate the victims' trust. Threat actors usually take a crisis as a favourable situation, and during this pandemic, they have outnumbered their previous records by targeting health and well-known government and international organisations, restricting them from doing their duty unencumbered.

A large number of work-from-home employees is another crucial target for cybercriminals to perpetrate attacks eyeing the enterprises. In such cases, the enterprises should strengthen their cybersecurity measures and spread cyber hygiene awareness to shield their businesses from infiltrators. At the same time, even consumers need to be taught how to protect themselves from such attacks and to always ensure good digital health.

Stay Home Stay Safe

Confidence in an insecure world

Copyright © 2020 K7 Computing Private Limited, All Rights Reserved.

This material has been compiled by K7 Labs. This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners. Email us at k7viruslab@labs.k7computing.com.

www.k7computing.com

