

April 2020

# COVID-19 crisis

The impact of cyber security on  
Indian organisations

The COVID-19 pandemic has caused widespread business disruption worldwide. We now live in a changed world where one of the most used strategies by organisations today is improvised business continuity through remote working. An effective strategy to protect business interests and expedited and large-scale movement in the physical workplace makes organisations more vulnerable to cyberattacks. Organisations are currently facing an increasing number of cyberattacks while they continue with their operations in this challenging environment. PwC's Cyber Security team has analysed the cyberattacks on Indian organisations in the last few weeks. The analysis is based on the pattern of attacks observed across a wide cross section of Indian organisations and has been done using data collected through logs and various other sensors.

Our analysis shows that there has been an unprecedented rise in the number of cyber incidents in the last few weeks as hackers aim to explicitly exploit the COVID-19 crisis. Various incidents of cyberattacks during the ongoing crisis have been widely discussed in news articles, columns and blogs. The figure below summarises the timeline and the various threat scenarios that are being used to exploit the vulnerability of organisations in these trying times.

The purpose of this threat landscape analysis is to decode the attacks and the attack patterns affecting organisations in India in the wake of the COVID-19 crisis. This analysis is based on the information collated from PwC India's cyber protection centres and covers data across industries such as manufacturing, financial services, e-commerce, information technology (IT), IT enabled services (ITeS) and others. It is also based on aggregated data and represents a general trend of cyberattacks being carried out against a cross section of Indian organisations.



## Timeline of cyberattacks exploiting the COVID-19 crisis

### January 2020

Coronavirus-themed malspam emails were used to distribute malware and Trojans, especially the Emotet banking Trojan.

### February 2020

- Phishing emails were designed as communication from the Centers for Disease Control and Prevention (CDC) to steal email credentials.
- COVID-19-themed phishing emails targeted manufacturing, finance, transportation, pharmaceutical and cosmetic industries.
- North Korea's BabyShark malware was spread via a document disguised as South Korea's response to COVID-19.
- Spam emails purportedly from the Center for Public Health of the Ministry of Health of Ukraine delivered a lure document containing the latest news about COVID-19, but in reality dropped a C# backdoor.

### March 2020

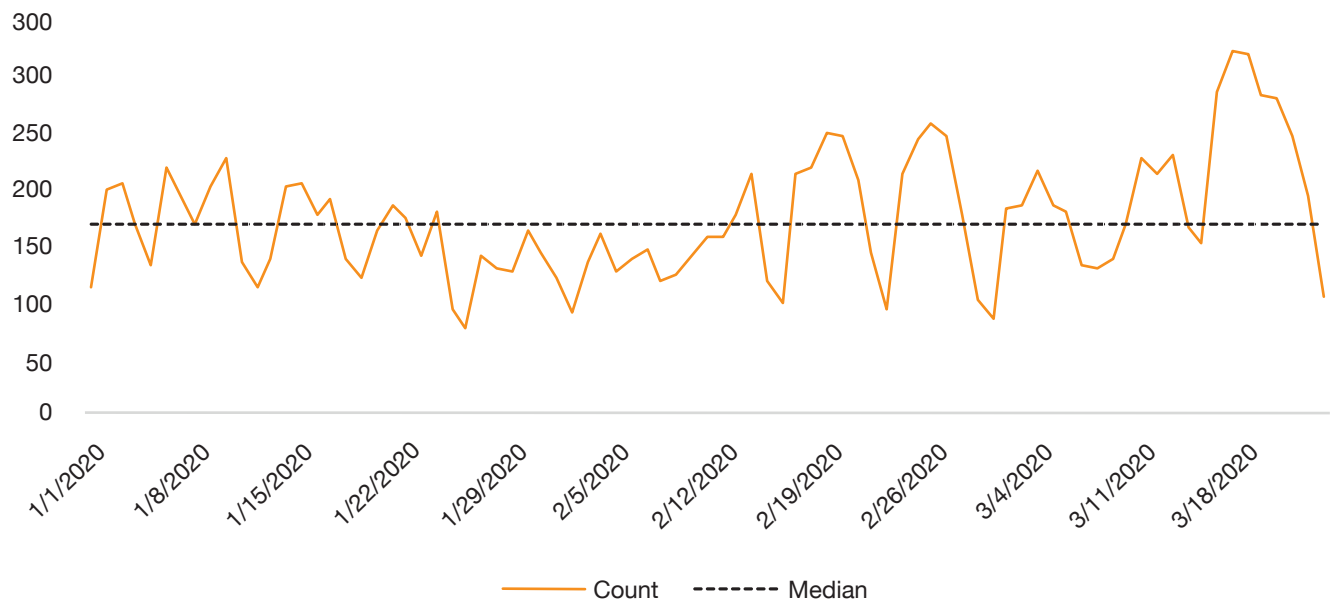
- Spam emails, camouflaged as a list of precautions against the coronavirus disease, targeted Italian email addresses to deliver a weaponised Word document embedded with a VBA script that ultimately dropped a new TrickBot variant.
- Cybercriminals exploited users' need for data about the coronavirus by implanting an AZORult payload inside an online application masquerading as an interactive map showing the spread of the novel coronavirus globally.
- A new ransomware strain dubbed as CovidLock was disguised as a coronavirus tracking app and distributed.

Source: PwC analysis

**As the COVID-19 outbreak reached India, the number of cyberattacks on Indian organisations doubled in March 2020 from January 2020.** The current crisis gives hackers and threat actors the most suitable opportunity to launch cyberattacks as countries worldwide are busy dealing with the pandemic. They are utilising this opportunity to exploit organisations.

There was a sudden spike in cyberattacks on Indian organisations in February 2020. A majority of these attacks were focused on exploitation of vulnerable services and obtaining easy access to remote desktops. Reports also came in about untargeted phishing campaigns in which the attackers impersonated personnel from various agencies engaged in combating the COVID-19 crisis. These were the two primary sustained waves in February 2020, after which the attack volumes fell back to a median level.

 Volume of attacks experienced



Source: PwC India Cyber Protection Centre

Post 15 March 2020, when India started witnessing a rise in the number of COVID-19 cases, there was a massive wave of attacks targeting many Indian organisations. This was a longer and sustained attack wave which later seemed to ebb but was quickly followed by a next set of attacks, as the figure above suggests. Typically, a spike in attacks or a mass cyberattack campaign in India quickly rises and falls within an average of 24 hours. A sustained campaign is known to occur at periodic intervals of a week or a few days. Many Indian organisations saw 100% increase in attacks between 17 and 20 February 2020. These attacks were wide-ranging and encompassed several threat vectors and sectors.

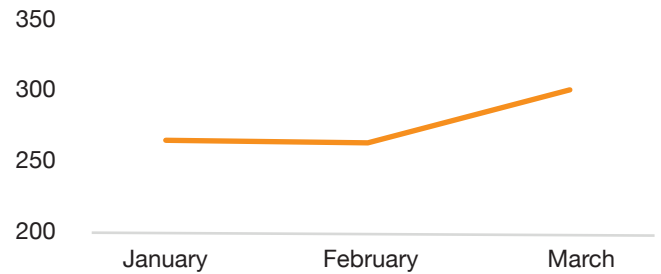


**The remote work infrastructure is being heavily targeted, along with attempts of identity theft and malicious payload delivery.** As organisations work in an expedited manner to set up virtual private network (VPN) infrastructure so that their employees can work remotely, threat actors are banking on weak authentication mechanisms and identity thefts through widespread phishing campaigns.

There has been a global spike in the number of phishing emails since February 2020, indicating a serious and targeted attempt to obtain credentials or deliver Trojans by exploiting human anxiety related to the COVID-19 outbreak. Phishing domains resembling the Centres for Disease Control and Prevention cropped up significantly all over the world. Most of these attacks were untargeted and designed to entrap a large number of users within the least possible timeframe. The global increase in phishing corresponded with the COVID-19 themed attacks.



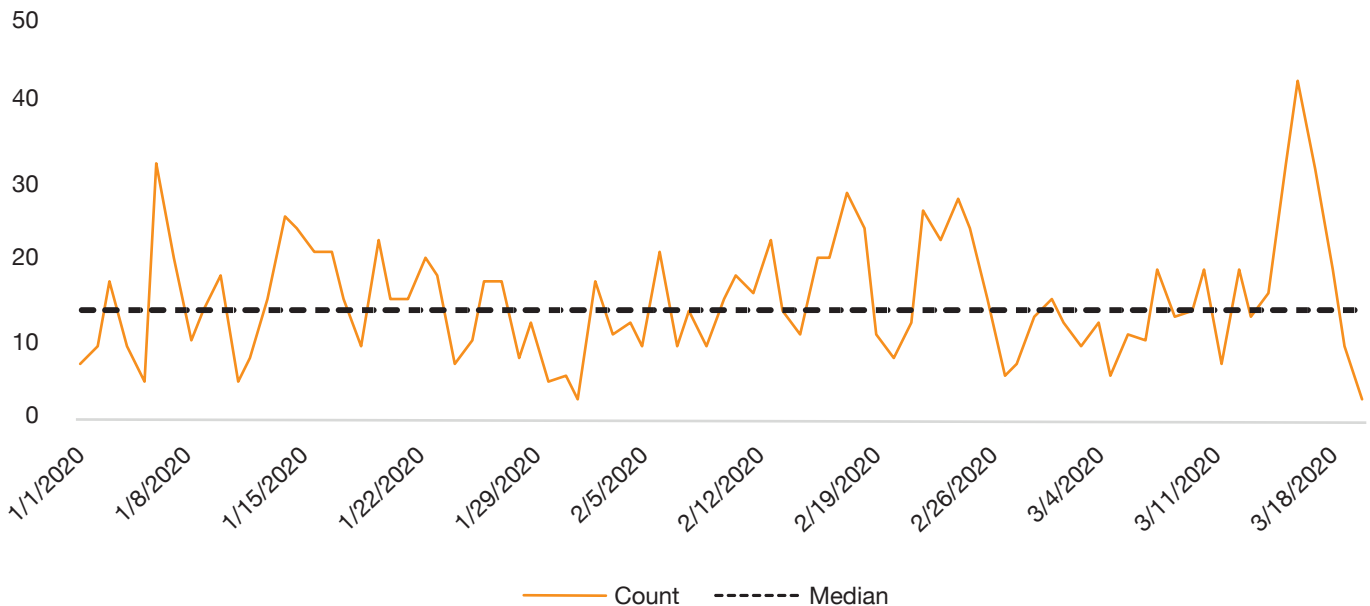
### Global volume of phishing emails (in billion)



Source: Cisco Talos



### Unique brute force attempts



Source: PwC India Cyber Protection Centre

Our analysts also observed an increase in brute force activity across our clients' systems during this period. Such activity peaked between 15 and 19 March 2020 and unique brute force attempts increased by about

300% over the median. Interestingly, there was a large number of failed logon attempts during this period, both in the organisational authentication mechanisms and VPN second-factor authentications.

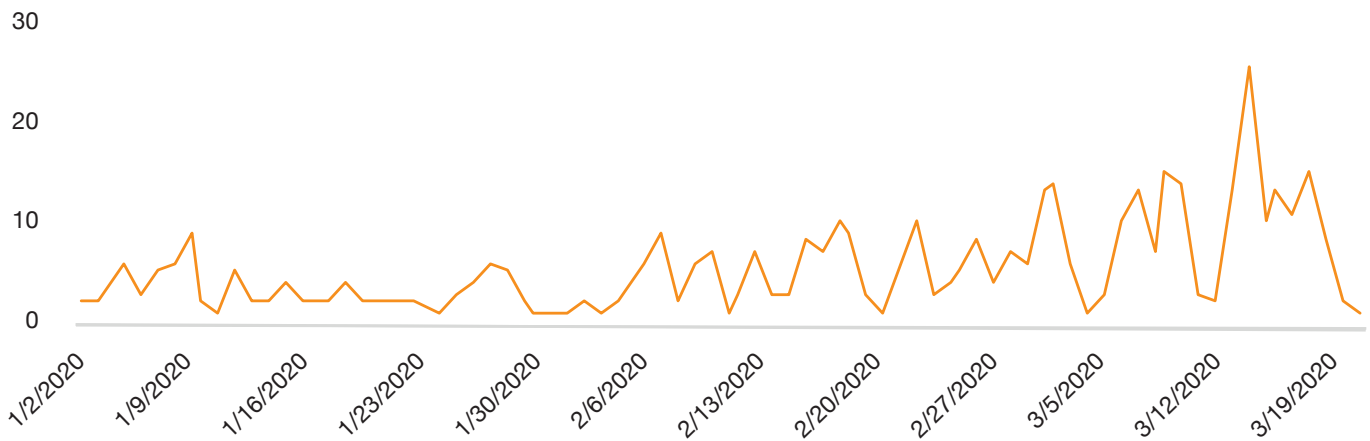


While the attempts to breach perimeter and remote access infrastructure were the primary motives of this attack, our analysis shows numerous attempts were made to deliver malicious payloads, including those related to the COVID-19 crisis. The major threat vector observed in India is AZORult – a malware designed to steal information, including credentials. This malware has been in existence for over three years but has recently been associated with malicious files and applications about COVID-19. Apart from malware related to COVID-19, there has been a steady rise in the number of incidents being detected by endpoint detection and response (EDR) systems across many organisations. The increase in EDR systems may or may not be directly attributed to the cyberattacks during the COVID-19 crisis, but it could have resulted from decreased patch compliance, increased number of people working remotely and use of unsafe devices connected to corporate networks through the provision of home VPNs in certain cases.


The critical indicators for cyber threats are increased volume of attacks, higher number of brute force attempts, theme-based phishing campaigns and increased EDR detections, which are all being triggered simultaneously and are causes of concern for organisations and their customers.



### EDR detection



Source: PwC India Cyber Protection Centre



IT and security teams across organisations need to synchronise their actions effectively to enable the safe continuity of business operations during the current crisis. Amongst the organisations we studied, the ones which dealt better with cyberattacks had:

- anticipated that the situation would deteriorate and planned for remote infrastructure in advance with due consideration for security implications
- already implemented security detection and response mechanisms that enabled them to anticipate the increase in threats and were agile enough to implement additional monitoring mechanisms early on
- tested various resilience and security controls ahead of time.



Considering the current threat landscape, organisations that have implemented remote working policies also need to implement robust preventive and detective technical measures. We recommend that they implement the following measures.



## Protection

- Utilise only secure access mechanisms for remote access – SSL VPN, secure remote desktop protocol (RDP) gateway, thin client access, etc.
- Implement strong password policies and two-factor authentication for all remote access, including those for administrative purposes.
- Review any exceptions to password policies, policy bypass and non-standard access.
- Review bring your own device (BYOD) policies and enforce compliance around patches, malware signatures and BYOD devices.
- Implement geo-restrictions and login velocity restrictions, if possible.
- Prevent multiple sessions and reuse of tokens wherever possible.
- Enforce privilege identity management solutions for remote administrative access.



## Detection and response

- Implement specific monitoring rules to detect attacks on remote access infrastructure.
- Utilise specific threat intelligence to detect threat actors targeting COVID-19 and related themes.
- Use EDR solutions, antivirus (AV) or authentication policies to isolate any infected or compromised endpoint.
- Enable response teams to securely access compromised devices for analysis and eradication.
- Identify mechanisms to re-flash operating systems where eradication is not possible.

**In the long term, we recommend that organisations focus on:**

- developing a robust business continuity plan (BCP)
- developing strategies and the required infrastructure for implementing secure remote access
- training technology staff and crisis management teams to enable smooth functioning of the BCP
- conducting tabletop drills and testing of crisis management plans
- communicating with various business teams and enabling them to continue with their functions in a secure manner.



# About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com](http://www.pwc.com).

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit [www.pwc.in](http://www.pwc.in)

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

© 2020 PwC. All rights reserved.

## About us

PwC's cyber security teams have vast experience in working with organisations, law regulators, international bodies and governments worldwide to help them prepare for and respond to cyber security issues during crisis situations and further enhance their cyber security capabilities for secure management of their operations.

Please write to Ashish Bhugra, our Cyber Security Director, at [ashish.bhugra@pwc.com](mailto:ashish.bhugra@pwc.com) for further details.

## Authors

### **Sangram Gayal**

Partner, Cyber Security  
PwC India  
Mobile: +91 98191 97716  
[sangram.gayal@pwc.com](mailto:sangram.gayal@pwc.com)

### **Parth Maniar**

Associate Director, Cyber Security  
PwC India  
Mobile: +91 96623 55555  
[parth.maniar@pwc.com](mailto:parth.maniar@pwc.com)

**pwc.in**

Data Classification: DC0

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2020 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

GM/April 2020/M&C-5405

