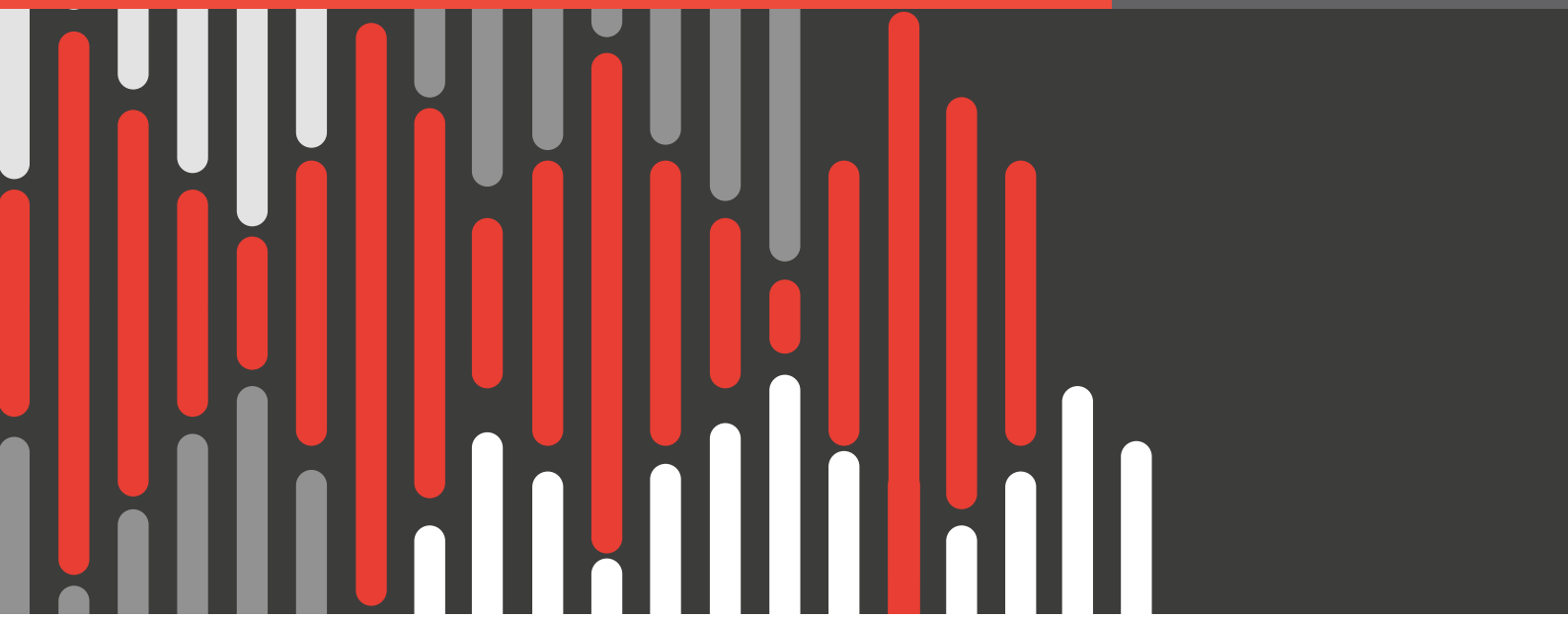
Managing the impact of COVID-19 on cyber security

Friday 20 March 2020



pwc

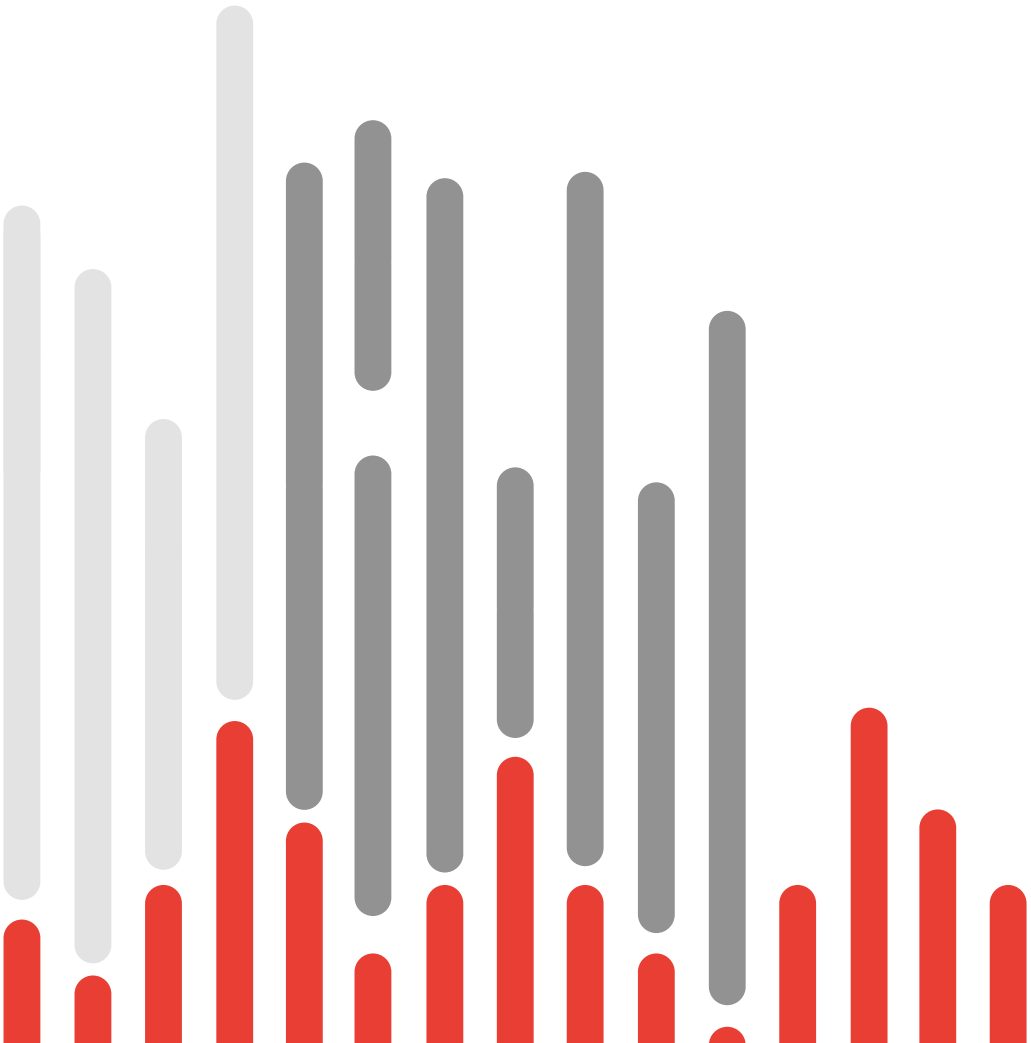
Contents

Managing the impact of COVID-19 on cyber security 1

What immediate impact may organisations face as a result of COVID-19? 2

How could this impact an organisation's cyber security risk? 3

How could organisations mitigate these risks? 5



Managing the impact of COVID-19 on cyber security

The COVID-19 outbreak has been declared a pandemic by the World Health Organisation, causing huge impact on people's lives, families and communities. This has had an immediate effect on organisations, changing the ways employees work and bringing with it new cyber risks.

As the international response continues to develop, we know that organisations are facing potentially significant challenges to which they need to respond rapidly. Many organisations and employees are needing to rethink ways of working in light of considerable operational and financial challenges. Without appropriate considerations, this could fundamentally increase the risk of cyber security attacks.

We are seeing both the likelihood and impact of cyber attacks increasing and cyber security good practices may fall by the wayside as organisations become more technology dependent than ever. We are also beginning to see the nature of the threat changing, as attackers exploit uncertainty, unprecedented situations, and rapid IT and organisational change.

Organisations should take three key actions to mitigate these emerging risks:

1

Secure their newly implemented remote working practices.

2

Ensure the continuity of critical security functions.

3

Counter opportunistic threats that may be looking to take advantage of the situation.

What immediate impact may organisations face as a result of COVID-19?

As a result of COVID-19 we are likely to see many organisations facing challenges including:

Maintaining business operations will be prioritised in a culture of crisis.

Priorities will shift as many organisations prepare for, or experience, significant financial and operational challenges. This may lead to IT and cyber security being deprioritised, with budgets being cut or at least their future being uncertain and hiring freezes put in place. This may affect planned security and IT improvement programmes and could delay important activities, including those that make organisations more resilient to cyber threats.

Higher numbers of the workforce will be absent and efficiency may decrease.

As COVID-19's impact on society increases and infection rates rise, higher numbers of the workforce are likely to be absent, especially as we head into peak periods of infections. Those who remain are likely to be less effective due to an increase in additional pressures, or general worries about the situation.

The workforce will rapidly shift to remote working and require technology to support this.

Shifting to remote working at both scale and pace is likely to cause significant impact, changing both IT infrastructure requirements and the attack surface. This will cause significant pressure on security teams, who may be refocused to support general IT operations, or to rapidly modify processes and technologies to adapt to changing risk.

Critical suppliers will be disrupted, potentially interrupting crucial security activities.

Organisations' supply chains will also be impacted and this may lead to disruptions in service provision. This is likely to include critical elements of the security supply chain, for example, outsourced Security Operation Centres, patching, and firewall management teams.

Organisations will become increasingly reliant on remote access technology, including technology their employees are not familiar using.

As organisations move away from their physical premises, and become increasingly reliant on remote access technology, any disruption caused by cyber security attacks or IT outages will have a significantly greater operational impact. Furthermore, the usual manual or physical workarounds used to overcome these issues may be unavailable.

How could this impact an organisation's cyber security risk?

We expect that many initial organisational responses to COVID-19 will have a net-negative impact on the cyber security posture of the business. This will be both as a result of existing risks being left unaddressed as security expenditure is cut and IT changes are frozen, and as we see new risks emerging.

A shift to remote working and prioritising business operations will bring immediate risks

Security controls may not be applied to new systems or tools hastily stood up to support employees with remote working that 'just works'. Security teams may not be consulted on systems before they are deployed, or exceptions will be put in place for assurance activities normally carried out (e.g. penetration testing). This will result in controls not being applied and less effective detection capability on these systems.

Existing processes and good practices may be sidestepped by, or not available to, employees when they encounter obstacles to normal ways of working. For example, workers finding their normal secure method of sharing files is unacceptably slow when working from home, may resort to using free and unsanctioned services as an alternative. Workers may also not have access to secure methods of document destruction in their homes.

Employees may be more susceptible to social engineering attacks as attackers take advantage of employees' increased workloads, unfamiliar ways of working and heightened stress levels. Phishing attacks crafted to exploit potential alarm around COVID-19 have already been seen in action. Widespread remote working will cause employees to rely on non-verbal ways of interacting with colleagues, meaning that existing informal methods of confirming the legitimacy of communications are less likely to be effective.

Reliance on remote access systems may make organisations more vulnerable to distributed denial of service (DDOS) attacks. Maintaining reliable remote access systems will become critical to business operations, as employees work remotely. Remote access systems may be targeted by attackers with denial of service attacks, seeking to disrupt business operations or to extort money.

Employees will be required to work with technologies they are not familiar with, potentially resulting in new security risks being introduced. Employees will likely be required to work with unfamiliar technology (e.g. remote collaboration tools) under increased levels of stress and while working in a way they are unaccustomed to, where opportunities to provide sufficient training may have been limited. This could introduce new risks as technologies are used inappropriately, are misconfigured or are not used with the security measures that were envisioned when they were designed.

Disruption to the workforce and suppliers will increase vulnerability to old risks

Vulnerabilities may be introduced as security basics such as patching are neglected, due to resources being refocused elsewhere. Regardless of global events, security vulnerabilities continue to be discovered in IT systems and continuous efforts are required to ensure these are addressed before attackers are able to exploit them. Neglecting these basics will compound vulnerabilities over time, and significantly impact security risk exposure.

Insider threats may increase as organisations face the prospect of having to make portions of their workforce redundant, or having to reduce working hours. Disgruntled employees facing redundancy may look to remove intellectual property, gain financially or otherwise cause reputational or financial damage to their employers.

Organisations may not effectively detect cyber attacks as security teams are short-staffed or repurposed to support other activities, leaving security alerts uninvestigated. Organisations are also likely to struggle with detection as their Managed Security Service Providers will be unavailable as they manage disruption to their own workforce.

Organisations may not be able to effectively respond to and recover from cyber security attacks as key employees from security, IT suppliers, and the wider business may be unavailable to support decision making and response efforts. This is likely to be especially true for organisations with lower maturity who rely on key individuals, rather than having fully documented and widely rehearsed processes.

Going forward this will change organisations' cyber security risk landscape

Technologies tactically stood up to support remote working may become relied upon by workforces once the organisation has returned to business as usual. However, in the haste of getting these technologies into operation, they may not have been assured to the same security standards as other IT tooling. For example, laptops rapidly deployed to support remote working may lack essential controls such as full disk encryption, leaving the data stored on them vulnerable once the workforce becomes mobile again.

An organisation's response will likely have lasting implications on how its employees work, with the shift of more applications into the cloud to support changes. Remote working over the short to medium term will likely lead to changes in the behaviours and cultures of organisations going forward, and their approaches to remote working. Technology will be key to enabling this, with organisations likely moving more of their applications to the cloud for email, document collaboration and file storage. These technologies bring with them new risks, but also allow security teams to design in security from the start and move away from legacy IT.

However, we also expect that some cyber security risks are likely to be decreased as a result of changes. For example, a workforce operating from primarily home and travelling less will have a decreased physical security threat.

How could organisations mitigate these risks?

Organisations should take three key actions to mitigate these emerging risks:

1. Secure their newly implemented remote working practices.
2. Ensure the continuity of critical security functions.
3. Counter opportunistic threats that may be looking to take advantage of the situation.

We also recommend that organisations look, where possible, to implement quick-win security controls and maximise their ability to prevent, detect and respond to threats given the increased reliance on technology and potential for emerging opportunistic threats.

1. Secure newly implemented remote working practices

Monitor for shadow IT and move users towards approved solutions.

Review web traffic logs to monitor for the use of shadow IT (e.g. file sharing, video conferencing, and collaboration tools), and work to implement and move users towards business-approved and secured solutions (e.g. using Cloud Access Security Brokers and web proxy filtering).

Ensure remote access systems are fully patched and securely configured.

Review all remote access systems to ensure critical security patches have been applied and secure configurations have been used.

Identify any vulnerabilities or mis-configurations using penetration testing or red teaming.

Work with IT teams to integrate rapid and Agile security testing into the deployment of new remote access systems.

Secure configurations should also be applied to email, identity management (e.g. Active Directory) and conferencing systems used by remote workers, for example by disabling legacy authentication protocols.

Ensure on-premise security controls still apply to systems when they are not on the internal network.

Map out the network-centric border security controls that apply to devices when they are on the internal network and evaluate whether a similar control set still applies to network traffic from systems not on the internal network.

Confirm web browsing is secured by web filtering when working remotely and, if not, consider deploying a cloud-based web filtering solution to detect and prevent malicious web traffic.

Configure this to restrict the types of websites that can be accessed, restrict file types users can download and block access to newly registered or untrusted domains.

Confirm DLP and other security controls on laptops perform as expected when devices are removed from the internal network for extended periods of time.

Monitor remote access systems, email and Active Directory for anomalous logins.

Configure remote access solutions, email systems and Active Directory to log all authentication events.

Preserve logs and analyse these for anomalous activity, including brute force attempts, logins from unfamiliar locations, and logins that indicate impossible travel.

Monitor and react to issues encountered by employees with remote working.

Monitor the IT help desk to identify complaints from employees about processes, controls or technology limitations that are preventing them from working remotely. Collaborate with IT teams to respond to issues with agile fixes enabling employees to be productive and prevent them from bypassing existing processes.

Support your people to work safely and securely from home.

Your training provider should be able to push out a short 'working from home' training module to help the workforce understand the potential threats and safeguards they may need to take when working remotely. If not, try creating a short fact sheet or guidance note.

Importantly, let people know where they can go for any support and make it easy for them to consult and report concerns.

Review tactical actions and retrospectively implement key security controls which may have been overlooked.

Review any laptops or servers deployed to allow employees to work remotely, and ensure that they have key security controls including full disk encryption, anti-malware protection, data loss prevention, automated backup solutions and endpoint detection and response tooling applied.

Review new applications, tools or systems stood up to allow employees to work remotely, including cloud-based email and document collaboration systems (e.g. Microsoft OneDrive, Google Drive, Zoom, Skype), to ensure key security controls have been consistently applied.

Ensure remote access systems are sufficiently resilient to withstand DDOS attacks.

Security teams should work with IT to understand the resilience of remote access systems to DDOS attacks, including reviewing bandwidth available, limitations of remote access software and whether any DDOS protection services can be added in front of them.

In order to ensure resilience, organisations should also consider implementing a second remote access system for administrators to access critical internal systems in the event that the primary remote access systems are taken offline.

2. Ensure continuity of critical security functions

Organisations should prioritise reducing reliance on people, as well as maximising the use of process and technology to perform key cyber security activities.

Organisations should closely follow official medical advice, including on when the peaks in the number of COVID-19 cases are expected in countries. This will allow organisations to plan for these peaks and the higher numbers of employees likely to be absent from cyber security teams.

Identify and monitor critical security activities to ensure continuity.

Identify which activities are crucial to manage cyber security risk e.g. patching security vulnerabilities, security monitoring, identity management and backing up key systems.

Ensure sufficient resources are identified (with levels of redundancy) to deliver these critical services, and identify how leadership can monitor that these activities are taking place.

Confirm patching processes are functioning, including for laptops connected remotely.

Confirm patching processes still work when systems are not on internal networks and test that patches or updates applied will not impact on remote workers.

Ensure that plans in place for out-of-band patching are still valid and consider how remote access systems will be patched as they are now critical to business operations.

Perform continuous internal vulnerability scanning to confirm patching processes are functioning and all critical vulnerabilities have been patched or mitigated.

Secure Internet-facing applications and services.

Regularly audit and document Internet-facing systems and services, and ensure that any exposed systems and services are required.

Perform continuous internal and external vulnerability scanning to identify critical vulnerabilities in Internet-facing systems and ensure that any exposed systems and services are required.

Consider using cloud-based solutions to allow for rapid deployment and scalability, configuring regular scanning of internal and external services and web applications, and alerting for new external vulnerabilities and exposed services.

Implement IT change freezes on high-risk systems if normal processes cannot be followed due to workforce shortages.

Configuration changes to high-risk or commonly misconfigured systems (e.g. firewall access around cloud-hosted databases) should be restricted. Alternatively, additional approval processes should be put in place to ensure that changes are not made with insufficient consideration or in error.

Review how privileged users are going to perform administration.

Securing and segregating privileged access is key to preventing attackers from compromising high-value accounts and the wider network.

Many organisations use dedicated administrator terminals or privileged access management solutions to achieve this, and should ensure that these arrangements can continue remotely (for example, by provisioning additional laptops with more stringent security controls).

Organisations should also ensure that good security practices around administration continue to be upheld despite pressure to rapidly make changes across the IT environment.

Consideration should also be given to whether any backup methods for secure administration need to be put in place, for example if systems restrict administrator access based on IP ranges, this access may be disrupted if remote access systems go down.

Ensure you have the people, process and technology capability to detect and respond to cyber attacks.

Ensure teams have the people, processes and technology necessary to monitor and respond to alerts, with appropriate levels of redundancy. Consider augmenting Security Operations teams with additional resources, or procuring a managed service using Endpoint Detection and Response technology.

Also consider integration with automation and orchestration tooling, which can help reduce the reliance on people and ensure continuity despite reduced staff levels.

Update incident response plans and playbooks to ensure they function with a workforce primarily working remotely.

Review incident response processes (including frameworks, playbooks and runbooks) to ensure they are up to date, and function with a remote workforce.

Understand how to access endpoint telemetry and data remotely to support investigative work, and test that staff members in response roles have the access and training required.

Ensure that processes are also not overly dependent on key members of staff, and clearly describe actions which should be taken in the event of an incident so that less experienced staff members are able to implement them.

Deploy asset management tooling to ensure continued visibility as systems are moved away from the internal network.

Asset management tooling provides visibility of assets wherever they are and, crucially, shows whether they are compliant with security controls (e.g. whether systems are patched and running an updated version of the remote access client). Asset management tooling is key to ensuring security tools have full coverage deployed to all systems.

3. Counter opportunistic threats taking advantage of the pandemic

Target additional awareness and communications where emerging threats arise.

The support provided to staff regarding how to work securely from home should be reinforced, at the right time, with targeted communications about relevant emerging threats. This currently includes targeted phishing campaigns using COVID-19 lures, or highlighting to finance teams increased risks of business email compromise attacks which attempt to exploit different or new ways of working.

Communications should be supportive, helpful and reviewed by communications staff to ensure they are sent at the right time and use language that does not cause additional anxiety.

Create a 'single source of truth' for your organisation in relation to COVID-19 advice in order to limit the likelihood of individuals being enticed to click on other potentially malicious lures.

Provide specific guidance to employees to be extra vigilant when it comes to requests for personal or financial information, or requests to transfer money.

Specific guidance should be provided to employees to ensure they do not respond to email solicitations for personal or financial information, or requests to transfer money, as we are already seeing social engineering campaigns centred around COVID-19.

Finance teams should review payment protocols to ensure these remain robust in new working environments, and finance staff should be empowered to be diligent in validating any unusual payment requests from senior individuals e.g. by contacting them for confirmation on a separate, trusted communication channel.

Mitigate the increased risk of insider threats in the event of redundancy or termination.

Develop plans to rapidly restrict on-notice employees' access to systems and data, in order to reduce the risk of data being stolen or systems being damaged. As organisations may not be able to physically collect devices from employees, plans should focus on disabling logical access to physical devices, accounts, and systems within the network.

Consider implementing additional logging of at-risk employees, reviewing the actions carried out by these, and using targeted DLP policies to prevent the exfiltration of data.

Mitigate the increased risk of phishing with technical controls.

Given the increased risk at this time, consider implementing additional technical controls to reduce the threat from phishing emails. This should include configuring filtering technology to whitelist the file types users can receive in email attachments or download from the Internet, and enabling advanced email filtering solutions to identify suspicious emails.

Apply quick-win technical controls across the IT estate where possible.

Given the increased short-term reliance on technology and the potential for emerging opportunistic threats, organisations should also seek to deploy quick-win technical controls in order to reduce risk.

Key risks that controls should address are phishing emails, attackers executing malicious code on workstations and servers, and performing lateral movement.

Consider deploying or upgrading anti-virus to provide Anti Malware Scan Interface (AMSI) capabilities to detect the malicious use of PowerShell and VBA, restrict the files that can be executed by users on workstations (e.g. PowerShell, HTA, and CHM files), restrict the execution of PowerShell with constrained language mode, and limit or prevent untrusted Microsoft Office macros from being run.

The emerging COVID-19 threat landscape

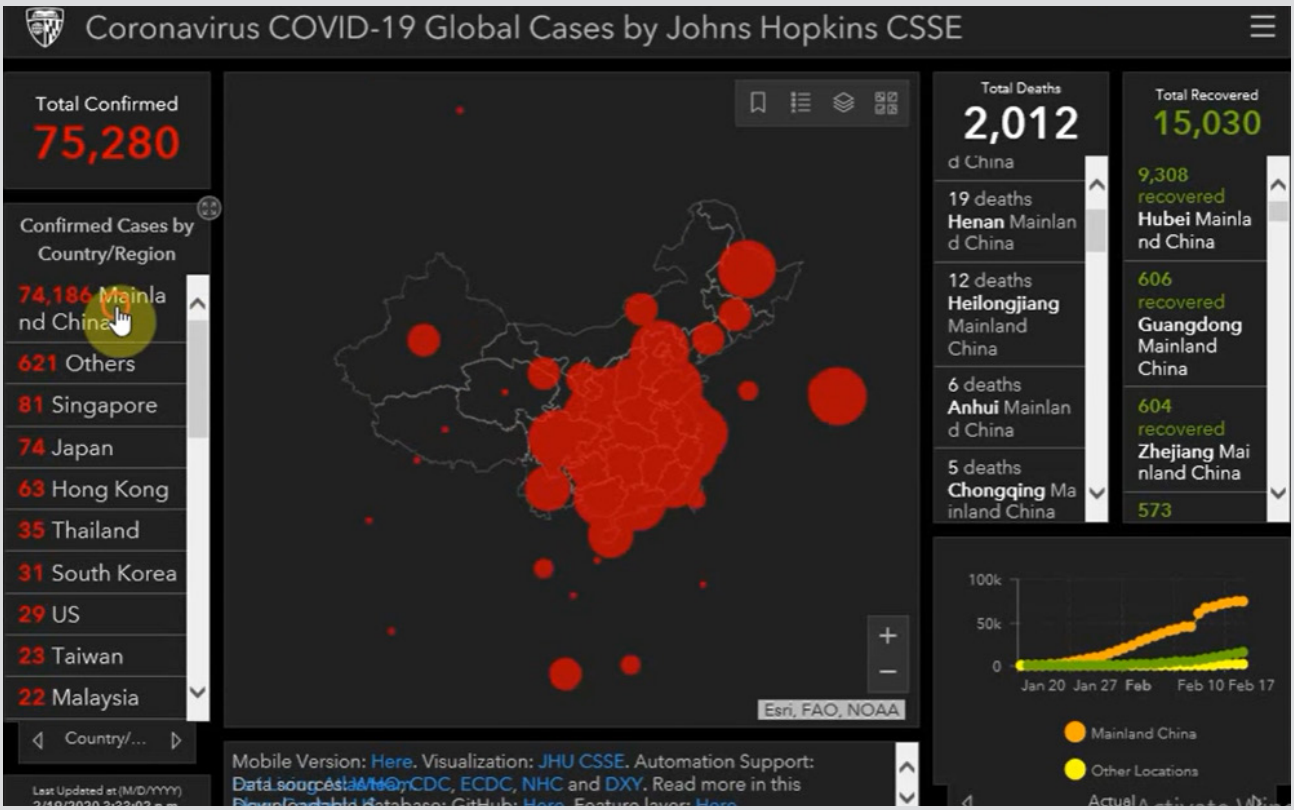
Threat actors are already exploiting the uncertainty and extraordinary response caused by the **COVID-19 pandemic.**

The criminal threat actor behind Emotet, which provides malware delivery services to sophisticated criminal actors including TrickBot, Ryuk and Dridex, began using COVID-19 phishing lures in January 2020, while the crisis was still in its early stages.

Other actors have since followed suit, with hundreds of new COVID-themed phishing lures being created each day. Many use legitimate content to encourage recipients to download malicious attachments.

We have identified criminal and state-sponsored campaigns exploiting COVID-19 and anticipate that they will also use VPN and video conferencing software lures to take advantage of users unfamiliar with remote working.

Example of a recently created phishing site



Screenshot of a phishing kit and downloader package on sale in Russian-language criminal forums. It uses a legitimate, interactive map developed by Johns Hopkins University as a cover for dropping malware, including the AZORult information stealer. AZORult is sold on Russian-speaking criminal forums and harvests passwords, login data and stored browser information (e.g. payment card details) from infected devices.

Get in touch

China South

Kenneth Wong
Cybersecurity & Privacy Leader
PwC Mainland China & Hong Kong
kenneth.ks.wong@hk.pwc.com
+852 2289 2719

Kok Tin Gan
Partner
kok.t.gan@hk.pwc.com
+852 2289 1935

Danny Weng
Partner
danny.weng@cn.pwc.com
+86 20 3819 2629

Felix Kan
Partner
felix.py.kan@hk.pwc.com
+852 2289 1970

Patrick Wong
Director
patrick.cm.wong@hk.pwc.com
+852 2289 8280

China Central

Samuel Sinn
Partner
samuel.sinn@cn.pwc.com
+86 21 2323 2296

Chun Yin Cheung
Partner
chun.yin.cheung@cn.pwc.com
+86 21 2323 3927

Ramesh Moosa
Partner
ramesh.moosa@cn.pwc.com
+86 21 2323 8688

Tony Wan
Partner
tony.wan@cn.pwc.com
+86 21 2323 8149

Sean Pan
Director
sean.pan@cn.pwc.com
+86 21 2323 2693

China North

Lisa Li
Partner
lisa.ra.li@cn.pwc.com
+86 10 6533 2312

Ryan Yao
Partner
ryan.h.yao@cn.pwc.com
+86 10 6533 7576

Dennis Li
Partner
dennis.y.li@cn.pwc.com
+86 10 6533 7800

pwc.cn.com