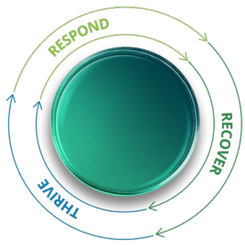
Issue 7| May 20, 2020

COVID-19 Global Cyber risks: Attack surfaces expand amid return to work efforts



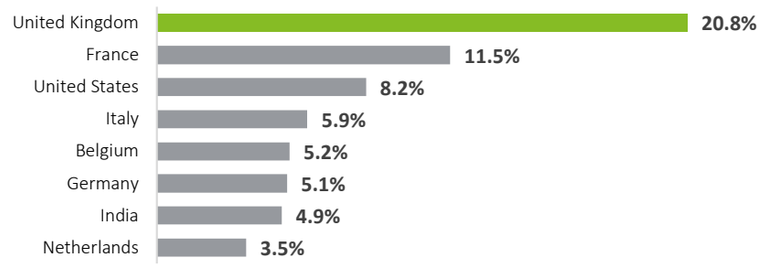
A bi-weekly high-level brief that focuses on some of the most current cyber threats and trends as identified by Deloitte Cyber Threat Intelligence (CTI), with near-term recommendations on managing cyber risks to respond, recover and thrive through the COVID-19 global pandemic.

Agile adversaries target all industries and geographies

In recent weeks, several countries have begun to ease their COVID-19 lockdown restrictions. Yet, amid the slow transition toward hybrid work environments that enable both onsite and remote work, pandemic-related cyber threats appear undiminished. Coronavirus-themed cyberattacks have now been confirmed in every country in the world.[1] Viruses have spiked on a year-over-year basis, rising 17 percent in January, 52 percent in February, and 131 percent in March.[2] **As this week's briefing shows, targeted attacks are also on the rise**—zeroing in not only on popular applications and platforms, but on industries across the board. With each passing week, the urgent need for heightened security vigilance, employee education, and a cyber risk-aware culture becomes clearer.

The Countries Targeted Most by Malicious Coronavirus Spam

In Countries targeted by largest share of global malicious spam emails with 'coronavirus' in the subject*



*January 1 to March 27, 2020
Source: Trend Micro, https://www.statista.com/chart/21291/countries-targeted-most-by-malicious-coronavirus-spam/

[1] Source: https://www.businessinsider.com/microsoft-research-shows-coronavirus-cyberattacks-in-every-country-2020-4
[2] Source: https://www.fortinet.com/blog/threat-research/preparing-for-the-surge-in-attacks-targeting-remote-workers.html

Be Aware: Bad actors are equal opportunity offenders. Anyone can be a target in COVID era

Targeted attacks on medical device suppliers

Impact reach: Medical, Healthcare | Geographies: Global

On May 1, 2020, Fortinet reported a spear phishing campaign launched against medical device suppliers. Featuring a subject line, "Inquiry on Medical Supplies", the spam emails requested information about the pharmaceutical and medical devices required to fight COVID-19. The email included a malicious attachment titled "Medical Inquiry – L.A.B. Equipment.doc" which, once opened, attempted to install a remote keylogger on the victim's system.

Targeted attack on US small businesses

Impact reach: All | Geographies: US

On May 8, 2020, a malicious spam campaign targeted US small businesses looking for COVID-19 relief funds. The spam emails appeared to originate from a legitimate US government email address, but were in fact sent from a compromised company domain. The email included an attachment that purportedly required the recipient's signature but actually contained a malicious file that allows hackers to control and monitor a Windows computer.

Targeted attack on South Korean manufacturing companies

Impact reach: Manufacturing | Geographies: South Korea

As part of the May 8, 2020 attack on US small businesses, cybercriminals also targeted manufacturing companies in South Korea. In this case, manufacturers received a spam email that purportedly came from the Centers for Disease Control and Prevention. The email included a malicious file that, once opened, gave hackers backdoor access to their victims' systems—enabling them to execute malicious commands, steal credentials, and log keystrokes.

Targeted attack on US accountants

Impact reach: Professional services | Geographies: US

A third email linked to the May 8, 2020 malicious spam campaign was sent to accountants in the US. The email claimed to contain COVID-19 related updates for members of the American Institute of CPAs. Recipients who opened the attached file extracted a remote access Trojan onto their systems that enabled hackers to steal user information and execute backdoor commands.

Attacks target popular collaboration platforms

Impact reach: All | Geographies: Global

For the week of May 6 to May 12, 2020, Deloitte CTI observed a series of new phishing campaigns targeting popular collaboration platforms that support remote workforces. In one instance, threat actors used fake certificate error notifications to trick users into sharing their Cisco Webex corporate credentials. In a related incident, fake login pages were created for Outlook and Office 365, enabling cybercriminals to steal user credentials once a victim unwittingly logs into the fake site. Trend Micro detected roughly 50,000 of these types of phishing instances between January and April 27, 2020 alone.

Mitigating actions to prevent cyber incidents

1. **Verify the email sender** through alternate communication methods and secure channels BEFORE opening. Avoid using any contact information provided in the message and do not click on attachments or open embedded links.
2. **Check that email** security gateways are fully deployed with advanced security capabilities, including the capacity to scan and block malicious attachments and embedded URLs.
3. **Install advanced email protection** tools that empower users to easily escalate threats, report phishing incidents, and flag other suspicious activity.
4. **Track host** and user activity to gain sufficient data for behavior-based analysis. This should help you identify suspicious threat actor activity or attempts to compromise hosts and/or user accounts.
5. **Devise a defined methodology** for Help Desk personnel to verify employee identification. This should help you reduce the risk of social engineering attempts that aim to reset passwords or take over accounts.
6. **Use Group Policies** to block users from enabling macros in Microsoft Office applications.
7. **Enforce heightened security protocols** for mobile devices.

Example:

A malicious Android app that claimed to track the spread of COVID-19 actually infected phones with ransomware.[3] This is a particularly salient threat as many countries (including Singapore, Australia, and the UK) have begun asking their citizens to install contact-tracing apps on their smartphones in anticipation of a return to work. These apps track people's movements so they can alert health authorities and anyone they've come into contact with if they begin showing symptoms or test positive for COVID-19.

While the apps themselves are raising privacy concerns, "fake" apps could cause even more damage—mandating heightened vigilance before downloading anything.

[3] Source: https://www.bbc.com/news/technology-52319093

Recover and thrive: COVID-19 underscores need for cyber risk-aware culture

With no end to COVID-19-related cyber threats in sight, organizations are coming to realize that they must strengthen more than their security technologies and policies. They must also foster an organizational culture that reinforces their cyber risk management program. Ignore the 'people component' and employees can become part of the problem, creating attack vectors for bad actors to exploit. This further underscores the need to cultivate a cyber risk-aware culture. Here are some of the basic principles:

Set the tone from the top. Because leaders model ideal behavior for an organization, it's up to leadership to set expectations for cyber risk management. To signal the priority of cyber risk-awareness, leaders should keep their finger on the pulse of emerging threats related to COVID-19, monitor cyber risk metrics pertinent to their business area, and elevate cyber risk to senior leadership discussions.

Continue to train. Employees who only received formal cyber training when they were onboarded likely need a refresher. Now is the time to push your training modules out through remote channels and mobile devices. If you have not yet done so, consider creating micro-training modules and gaming apps to make the learning more accessible and more memorable.

Get in touch. To reinforce your cultural priorities, send out regular communications from leaders, human resources, and other internal sources to address cyber risk issues and remind employees about your security policies and protocols. Aim to communicate through multiple channels, including email, text messages, videos, and collaboration platforms.

Revisit your vision. Under the strain of COVID-19, it may be time to update your vision for your cyber risk-aware culture. Are there new behavioral norms you now need to ingrain? Do you need to refine your cyber risk-aware practices? What cyber risk actions should employees be exhibiting right now (e.g., increased skepticism when receiving COVID-19-related emails, heightened consideration of cyber risks as they perform their operational tasks, escalating perceived risks…)?

Reward desired behavior. An organization's priorities are reflected in its talent lifecycle—how it hires, promotes, develops, and recognizes employees. To develop a culture that is cyber risk-aware, consider linking desired cyber risk behavior to performance management processes, publishing cyber risk metrics by business unit, or even crowdsourcing threat vectors.

We're by your side to help you through COVID-19

Relevant Deloitte Reads:

- COVID-19: Shaping the future through digital business
- Embedding trust into COVID-19 recovery
- COVID-19 Economic cases: Scenarios for business leaders

Deloitte Cyber drives progress in a dynamic, connected world, solving complex problems to build confident futures. Using human insight, technological innovation, and comprehensive cyber solutions, we manage cyber everywhere, so society – and your organization – can thrive anywhere.

Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com

Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca

Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk

Deborah Golden
US
+1 571 882 5106
debgolden@deloitte.com

James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au

Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@Deloitte.de

Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber