

The new era of WFH: *Staying Cyber Secure*

CFC Response and CFC Underwriting Ltd.

April 2020





Cyber

Pioneers in cyber insurance

With 20 years' experience in cyber insurance, CFC was one of the first companies to offer cyber insurance and has one of the largest cyber underwriting teams in the world. Our award-winning cyber insurance products are trusted by over 50,000 businesses in more than 65 countries.

CFC's dedicated in-house cyber incident response team is backed by a panel of expert global response partners and operates the world's first cyber incident response app.

Our cyber products

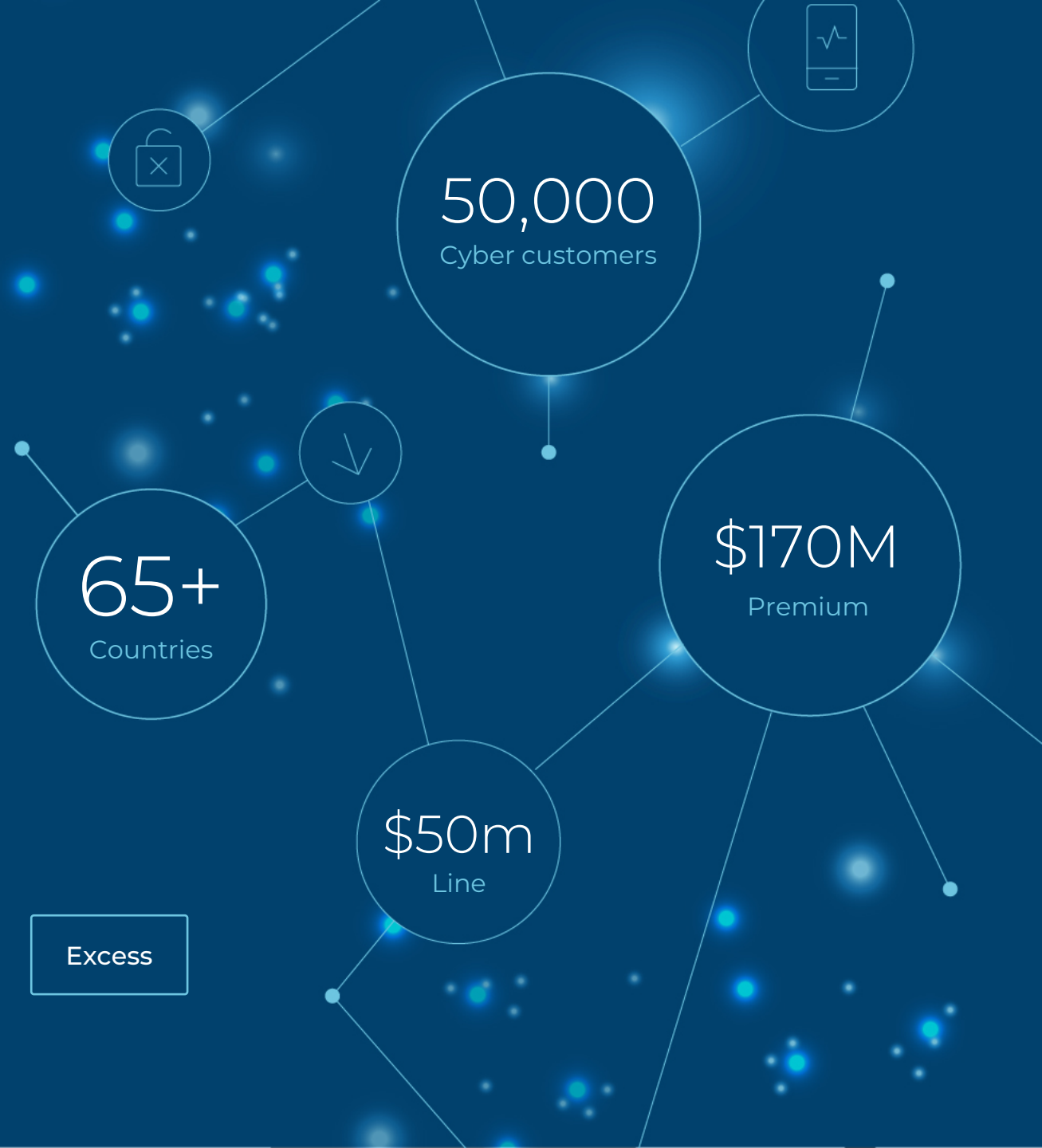
Private enterprise

Large corporate

Healthcare

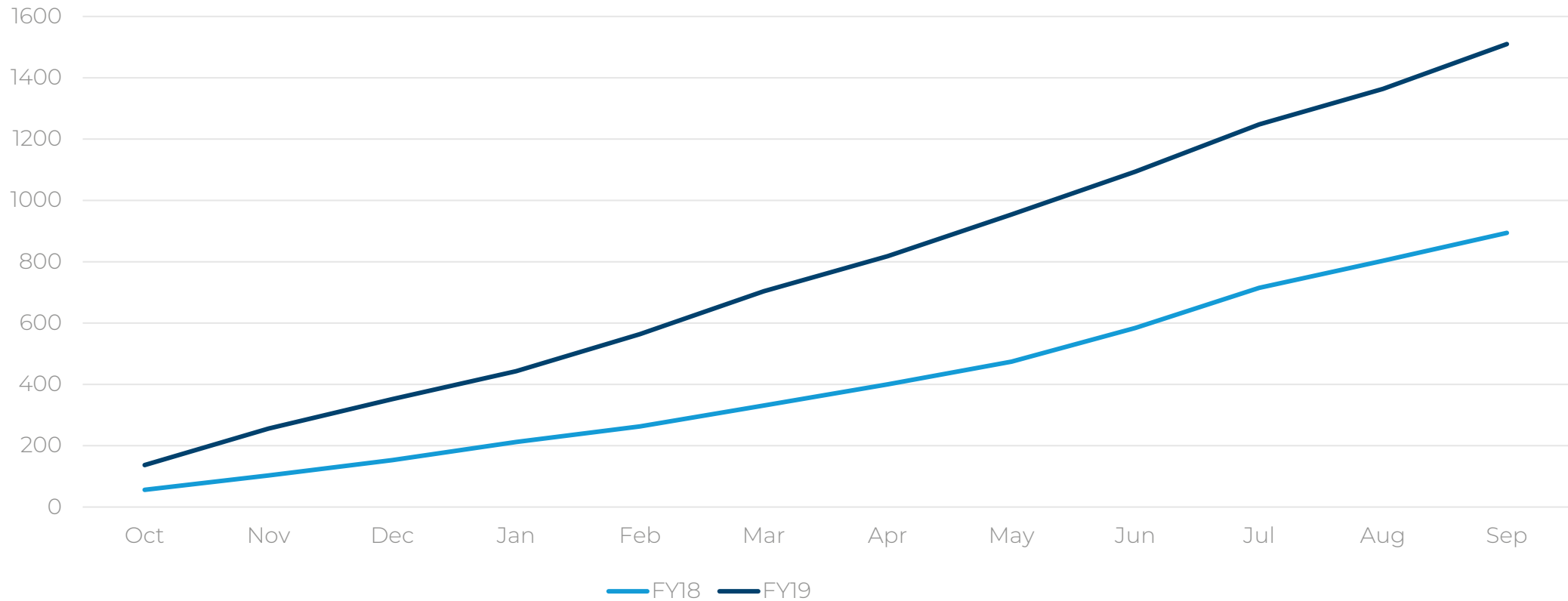
Excess

*Cyber cover is also offered as standard on most CFC policies

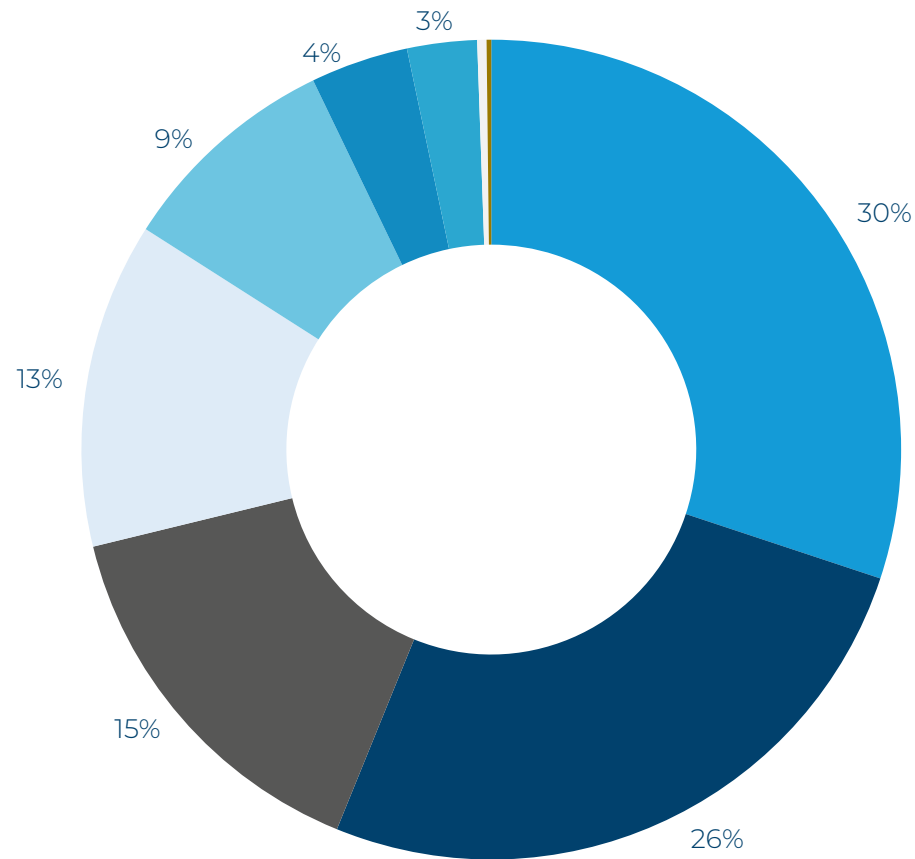


Cyber claims volume is up significantly on last year

Cyber claims volume TY v LY



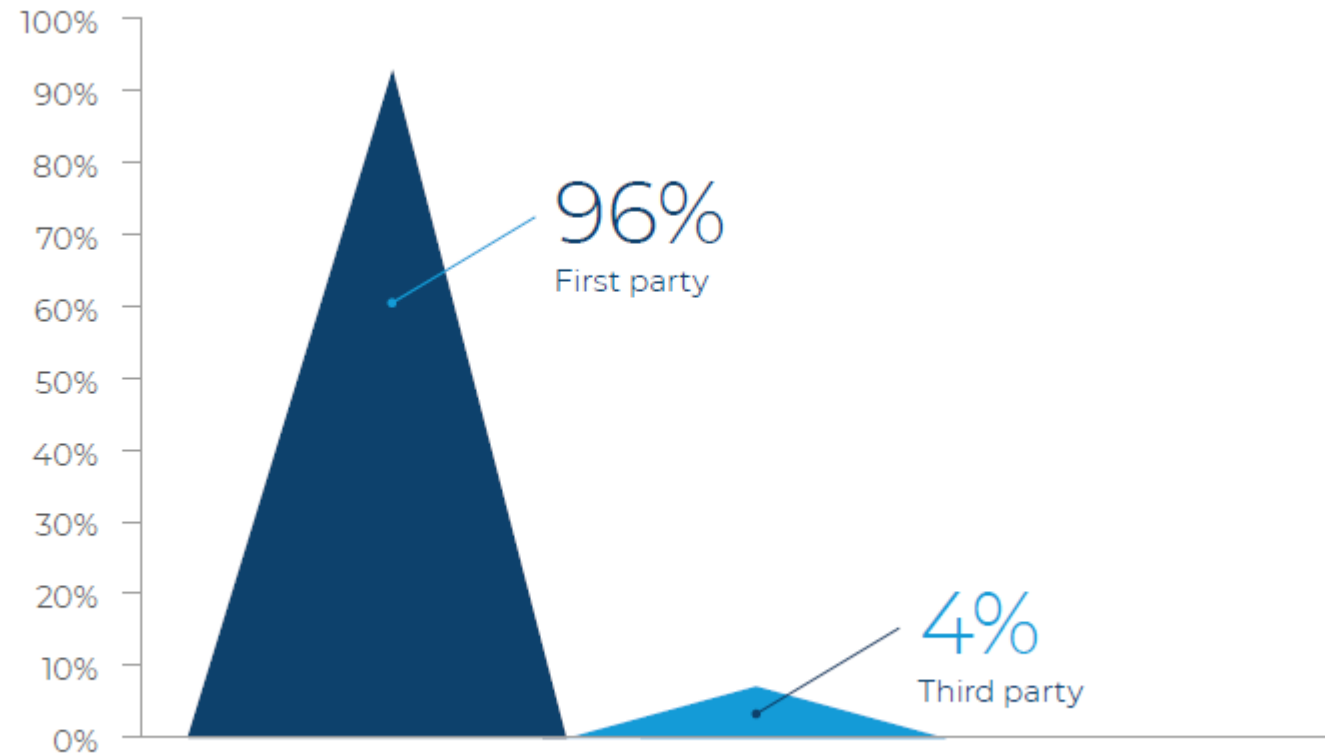
Cyber claims (by count)



All Countries

- Cyber (Ransomware)
- Cyber (Theft of Funds)
- Cyber (Data Breach – Hack)
- Cyber (Data Breach – Phishing)
- Cyber (Data Breach – Other)
- Cyber (Malware – Other)
- Cyber (Other)
- Cyber (IP Infringement)
- Cyber (Cyber Extortion)

First party v. third party claims



CFC Underwriting cyber claims statistics, 2018

Your CFC Team



Lindsey Nelson
Cyber Development Leader



Chris Loehr
Executive Vice President



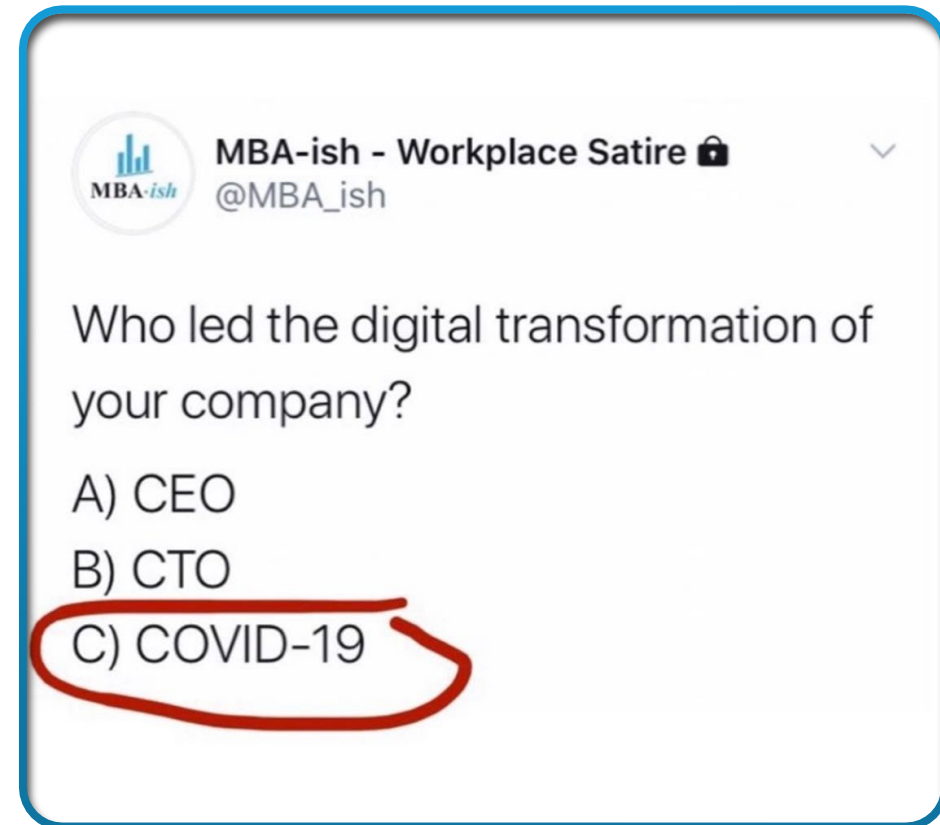
Brian Brown
Chief Security Officer



Remote Desktop Protocol 101

Remote Desktop Protocol 101

- VPN – Virtual Private Network. Allows companies to secure connections to other networks over the Internet.
- Remote access applications
- Pros and cons of using RDP or VPN
- The current most common cause of a Ransomware incident is compromise of remote access via Remote Desktop Protocol (RDP).
- What does that mean during COVID-19?

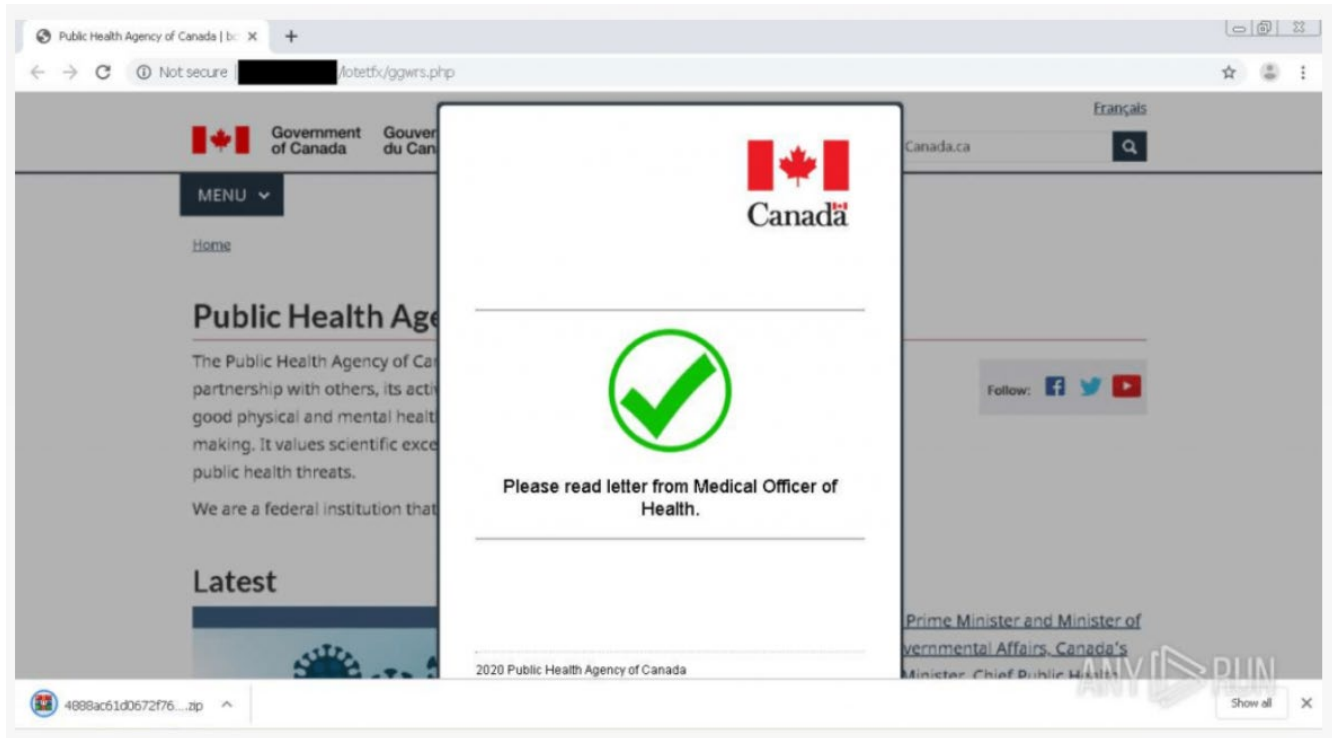




Top Five:
COVID-19

1. Posing as government agencies

- The website directs victims to download a file: “Please read letter from Medical Officer of Health”



Case Study: Remote Access Hacked

- Covid-19 forced a company to quickly come up with a plan for remote access
- IT Department created remote desktops on MS Azure to allow their employees to access the company without installing a VPN
- Employees used RDP to access the remote desktops with just their network username and password.
- Attackers were able to gain access with an employee's credentials
- Entire company was then encrypted
- **A lack of VPN and MFA is what allowed this to happen.**



2. Targeting food delivery – credential stuffing



Lieferando.de @lieferando

Online bezahlte Bestellungen, die auf Grund des Systemangriffs, nicht ausgeliefert wurden, werden so schnell wie möglich zurückerstattet. Bitte schickt uns eine Mail an info@lieferando.de

Translated from German by Google

Orders paid online that were not delivered due to the system attack will be refunded as soon as possible. Please send us an email to info@Lieferando.de

11:44 PM · Mar 18, 2020 · [Twitter Web App](#)

source: Lieferando



Jitse Groen @jitsegroen

A #ddos attack on a food delivery website @takeaway in the middle of a public health crisis. I hope you sleep well at night. @thuisbezorgd @lieferando @pysznepl

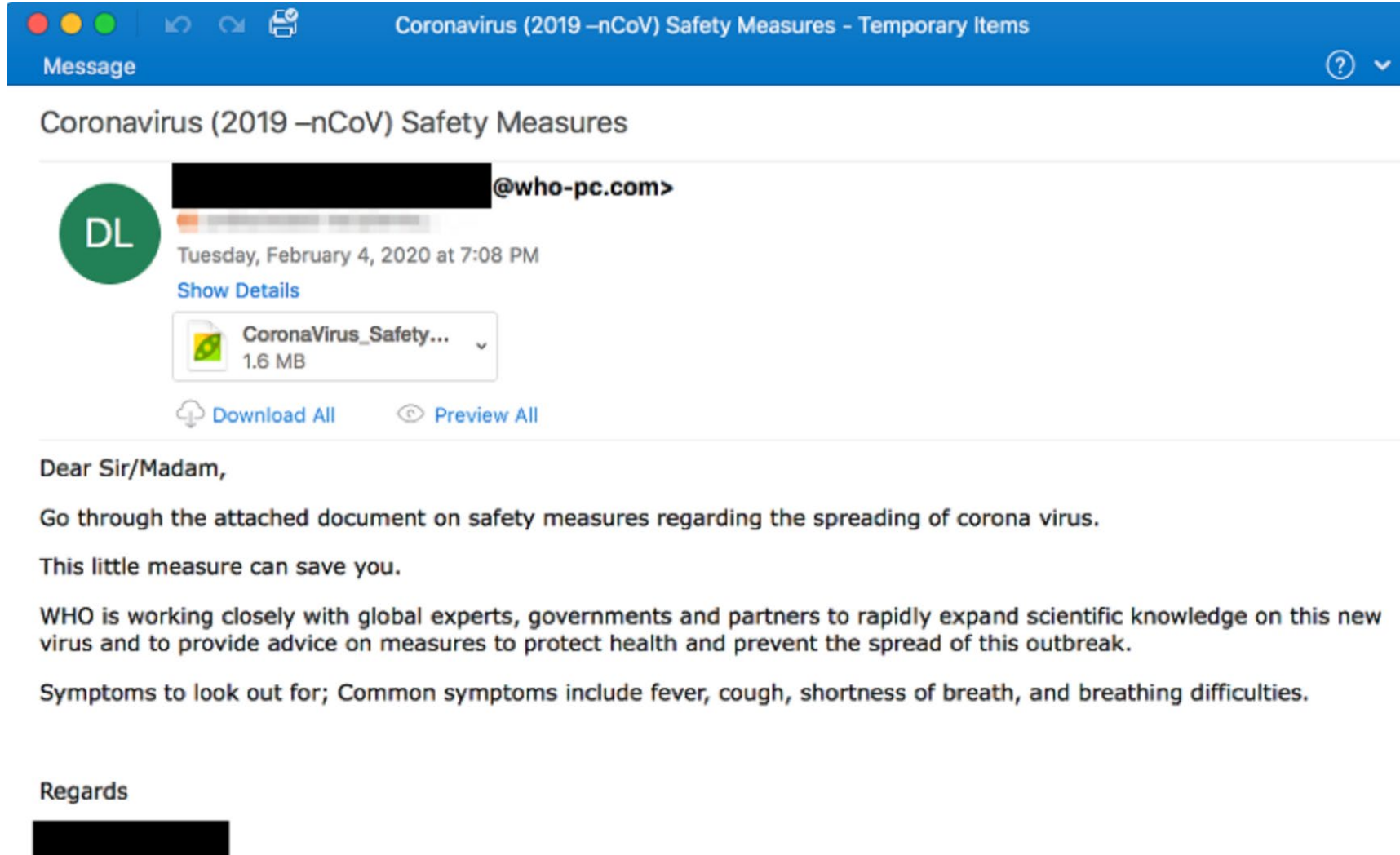
PIZZA.DE ➤

0054747 <0054747@protonmail.ch>
aan mij ▾

Hi, Jitse! Pizza.de is under attack.we want 2 BTC.tell me when you ready to pay. after payment we stop attack and help you to protect you company. we can attack another sites takeaway company.we waiting your answer.

7:40 PM · Mar 18, 2020 · [Twitter Web App](#)

3. Playing on human vulnerabilities




The screenshot shows an email interface. At the top, a blue header bar contains window control icons, the title "Coronavirus (2019 -nCoV) Safety Measures - Temporary Items", and a "Message" label with a help icon. Below the header, the email subject "Coronavirus (2019 -nCoV) Safety Measures" is displayed. The sender's information includes a green circular profile picture with the initials "DL", a redacted name, and the email address "@who-pc.com". The message is dated "Tuesday, February 4, 2020 at 7:08 PM" and includes a "Show Details" link. An attachment is shown as a document icon with the filename "CoronaVirus_Safety..." and a size of "1.6 MB". Below the attachment are "Download All" and "Preview All" options. The email body text reads: "Dear Sir/Madam, Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you. WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak. Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties. Regards" followed by a redacted signature.

Message


Coronavirus (2019 -nCoV) Safety Measures - Temporary Items

Coronavirus (2019 -nCoV) Safety Measures

 [Redacted Name] @who-pc.com

Tuesday, February 4, 2020 at 7:08 PM

[Show Details](#)

 CoronaVirus_Safety... 1.6 MB

[Download All](#) [Preview All](#)

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[Redacted Signature]

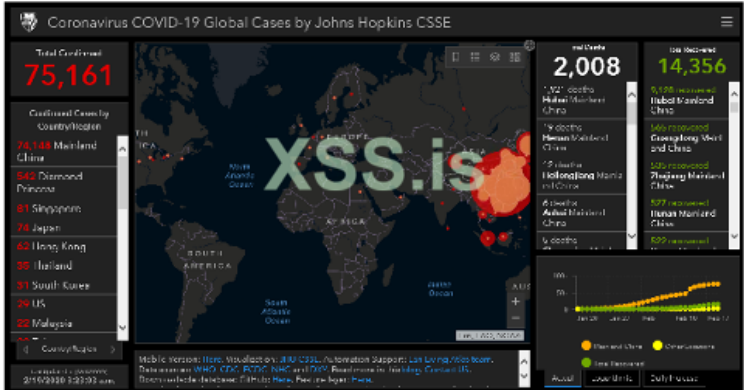
4. Creating malicious COVID-19 maps

[ПРОДАЖА] 👑 New Exploit and Corona Virus Phishing Method!
Zaher · 23.02.2020

23.02.2020

New Exploit and Corona Virus Map Phishing method
Новая Эксплоит плюс разводка с Карт распространения Корона Вирус

Zaher
флорру-диск
Пользователь
Регистрация: 17.02.2020
Сообщения: 5
Реакции: 2
Баллы: 3



The screenshot shows a web interface for a COVID-19 map. The map is titled "Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE". It features a world map with red dots indicating case locations. A large, semi-transparent "XSS.is" watermark is overlaid on the map. To the left of the map is a table of countries with their respective case counts. To the right is a summary of global statistics and a line graph showing the trend of cases over time.

| Country/Region | Cases |
|------------------------|-------|
| 75,161 Total Confirmed | |
| 74,148 Mainland China | |
| 540 Diamond Princess | |
| 81 Singapore | |
| 74 Japan | |
| 62 Hong Kong | |
| 35 Thailand | |
| 31 South Korea | |
| 29 US | |
| 22 Malaysia | |

Global Statistics:
Total Deaths: 2,008
Total Recovered: 14,356

Line Graph: Shows a steady increase in cases over time, with a legend for "China and China" and "Other countries".

Corona Virus is now in all news. And it get 10.000 newly infected every day with growing speed. This is hot topic now. Offered method allows to send a payload Preloader masked as a Map.

!!! PreLoader has file extension which **can be sent as attachment** by any mail service directly. **Can send to Gmail as attachment too!** See video example

5. Recruiting laid off workers for scams

- ❑ Recruitable “money mules” - roping the recently laid off into money laundering schemes
- ❑ “Coronavirus Relief Fund”
- ❑ Legitimate looking website for funding relief efforts
- ❑ Offices in Nebraska, U.S., and Quebec, Canada
- ❑ Content lifted almost entirely from [globalgiving.org](https://www.globalgiving.org)
- ❑ asked to process a “donation” from someone who wants to help fight the Coronavirus outbreak
- ❑ Job solicitations too good to be true





So what?

Personal Devices



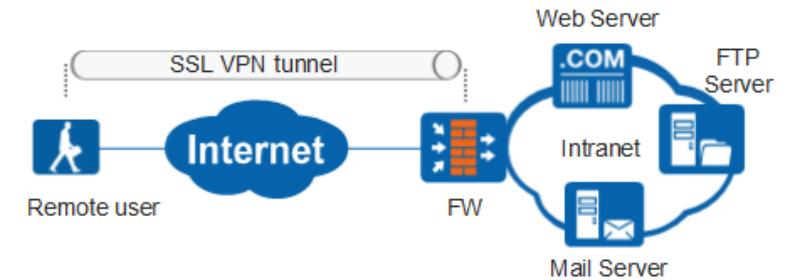
Multi-Factor Authentication

Google Authenticator
Microsoft Authenticator
LastPass Authenticator



Password Manager

1Password.com
LastPass.com



SSL VPN

Remote Access

Employee Training

DO:

- Ongoing security training for all remote workers
- Monitoring employees the right way
- Check all of your devices for software or firmware updates
- Use a unique password for every online login

DO NOT:

- Don't click suspicious links
- Don't download attachments from unknown or untrusted sources
- Do not "Enable Content" in unknown Word documents
- Be careful not to share login credentials with unknown or suspicious providers (there is NEVER a legitimate reason for a third-party to require your login credentials)
- Check all of your devices for software or firmware updates

Preparedness

Partnering with:

BITSIGHT **SKURIO** **Cyber Risk Aware** **NINJIO**

Want to protect yourself? Contact cyberservices@cfunderwriting.com

| Prevent | Detect | Respond |
|---|--|--|
|  <p>Phishing-focused training CyberRiskAware is an eLearning tool that tackles the human vulnerabilities in your business, equipping your team to identify and prevent phishing attacks and other social engineering campaigns.</p> |  <p>Cyber risk rating report Bitsight will review key features of your company's internet presence on request and provide you with a cyber security rating, allowing you to benchmark yourself against peers and competitors. This tool also gets you 30-day trial</p> |  <p>Cyber incident response planner CFC's incident response team delivers a unique toolkit combining multiple templates and practical advice to help you produce a tailored incident response plan in case the worst happens.</p> |

We're risk management fanatics



Incident Response Planning

- Update Corporate policies
 - Include plans for digital assets due to system failure or cyber events
- Know who in the company actually needs VPN access
- Test out incident response plan ahead of time – tabletop exercise
- How does the IRP work when everyone is remote versus in the office?
- Cyber insurance!



Client questions

Questions

Have you seen more targeted attacks by hackers now that bitcoin is half the value?

- The number of attacks we see has increased somewhat, but I wouldn't say that the increase is what we would have initially expected. What we have seen is the attackers who state their ransom demand in bitcoin versus USD have used the fact that bitcoin is low as a reason the victim should pay immediately "before bitcoin increases in price".

Questions

Are there any corporate VPNs that you recommend? Or any specific features to look for?

- Most of the major security/VPN vendors offer a very robust and reliable VPN solution. Most have optional features that an organization can choose to buy and implement. One of these features is to interrogate a computer to make sure it is patched, has good antivirus and possesses other security attributes before it is allowed onto the network. Another feature is to expand similar capabilities to mobile devices such as phones and tablets. What we see when we come across VPN issues is poor configurations. We see lack password controls, features not enabled that should be enabled and a lack of segmentation between VPN-connected computers and internal computers.

Questions

With regards to VPN, etc. if an insured is predominantly cloud-based, therefore doesn't have physical servers on site, but instead is relying on AWS and similar, what options do they have for increasing their security/prevention on attack?

- Moving systems to the cloud has its advantages that we don't need to go into. However, that does not eliminate the need for security. Most security controls that are required in traditional server environments can and should be implemented in the cloud. For example, VPN connectivity can be implemented in the cloud. It really comes down to what has been migrated to the cloud and how it is being used by your employees and customers. The risks need to be assessed and the proper security controls be designed, implemented and monitored.

Questions

You mention using a chat for company continuity, this is something that was brought up in our company yesterday. In particular using Discord. Is there much in way of risk or attack Vectors using a tool like this? Short of password reuse or weaknesses?

- Chat and collaboration applications have come under a lot of scrutiny lately and deservedly so. There has been a massive adoption and increase in the use of these tools due to the current situation. This has drawn the interests of security researchers and hackers alike. Any time an organization chooses to adopt a technology solution, it should be properly assessed prior to deciding to adopt it. Additionally, an organization should keep close tabs on any security reports about any application they use. This information is very easy to find and track and that can help protect an organization from using an application that is at risk.

Questions

Can you speak to the use of Password Vaults and the like?

- Password vaults, specifically well-known solutions that have enterprise features are recommended by us all the time. Until passwords are replaced with something effective and user-friendly, we all will have to continue to rely on strong passwords. A good password vault solution will give you the security around those passwords, give you the ability to generate randomized strong passwords, integrate with your browsers and mobile devices for ease of use. As with the prior question, an organization should assess the risk of the solution prior to adoption and understand how it should be configured and used by their employees to ensure effectiveness.

Questions

During the sound issues, whilst discussing the use of employees' own computers, and I think I heard online shopping mentioned - what was the risk here - was it just mixed personal and commercial use increases risk?

- The fact that is of mixed use complicates things more than increases the risk. When people use their personally-owned computers to access corporate resources, they may not use a separate profile on their computer to do so. So, if the organization gets compromised, anything and most probably everything on that computer, such as any saved passwords, will be compromised. The use of a password vault is recommended to store and use passwords versus saving passwords in a browser. If you use the “Save My Password” function on a website, those passwords are stored locally and can be at risk of theft.
- Note: When a mobile device such as an iPhone asks you to store your password, that is being stored in a password vault. We are only referring to doing it from within the browser when the website gives you that option.

What are their challenges?

- Were you able to switch to working remotely with minimum disruption?
 - Or, are you having to implement methods to access the office remotely?
- Are most software and services being used cloud based?
 - Or, are you having to look at migrating?
- Do you still have any legacy systems in your office?
- Do you know what your employees NEED to have access to?
- Is someone testing back-ups monthly?



The image features three overlapping circles in various shades of blue (light blue, medium blue, and dark blue) on a dark blue background. The text is centered horizontally and partially overlaid by the circles.

cyber@cfcunderwriting.com