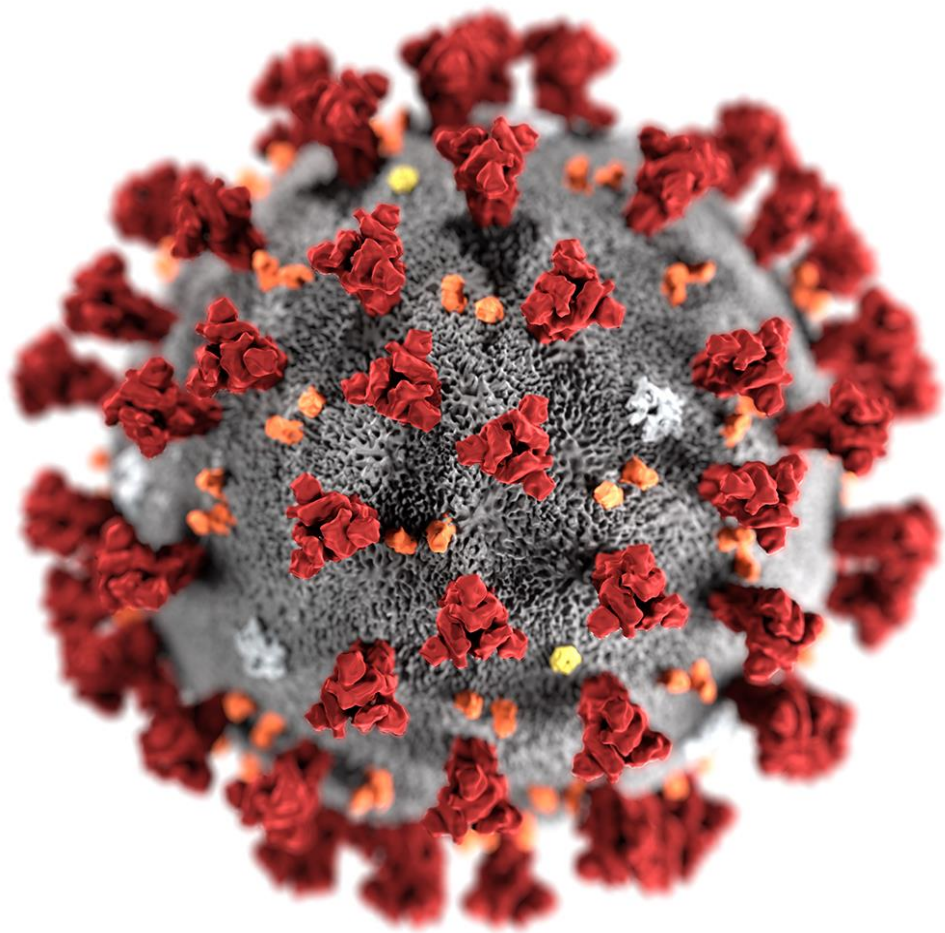




CYBERCRIMES IN THE CORONAVIRUS ERA

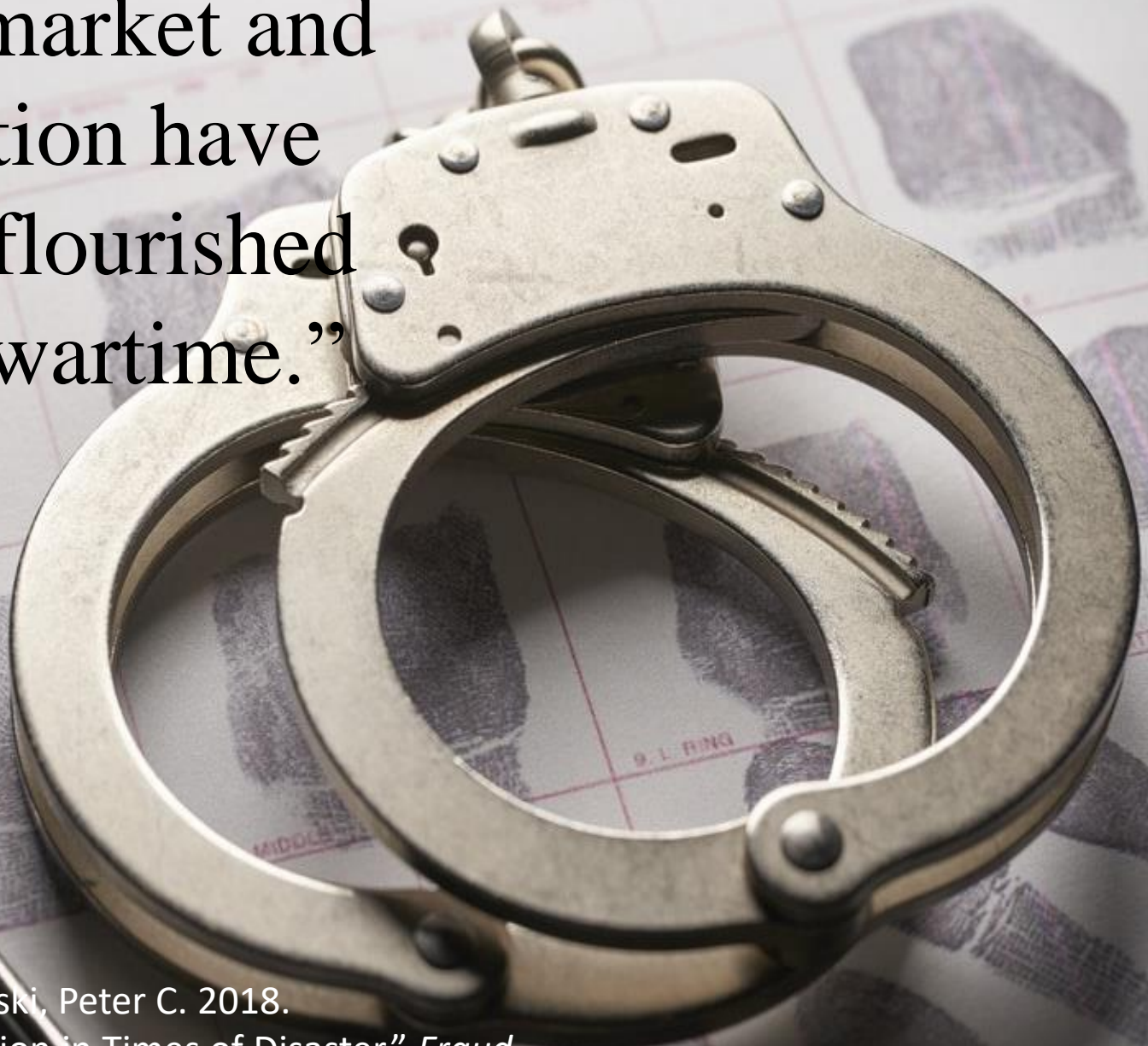
The Institute for Cyber Policy Studies
Cybureau.org | Tal@cybureau.org | +972-525-258-985







“Black market and corruption have always flourished during wartime.”



Kratcoski, Peter C. 2018.

“Fraud and Corruption in Times of Disaster.” *Fraud and Corruption* (Springer, Cham) 139-157.

doi:https://doi.org/10.1007/978-3-319-92333-8_8

POLL

During January 2020 there were 1,200 COVID19 related attacks.

How many did we see in February and March?

- A – February 2,400, March – 5,000
- B – February 580, March – 3,650
- C – February 10,000, March – 380,000
- D – February 3,400, March – 52,000

Overall threats seen in the Zscaler cloud

85% increase in phishing attacks targeting remote enterprise users

25% increase in malicious websites and malware files blocked

17% increase in threats targeting enterprise users

What a difference three months makes
Jan. vs. March

COVID-19 threats seen in the Zscaler cloud

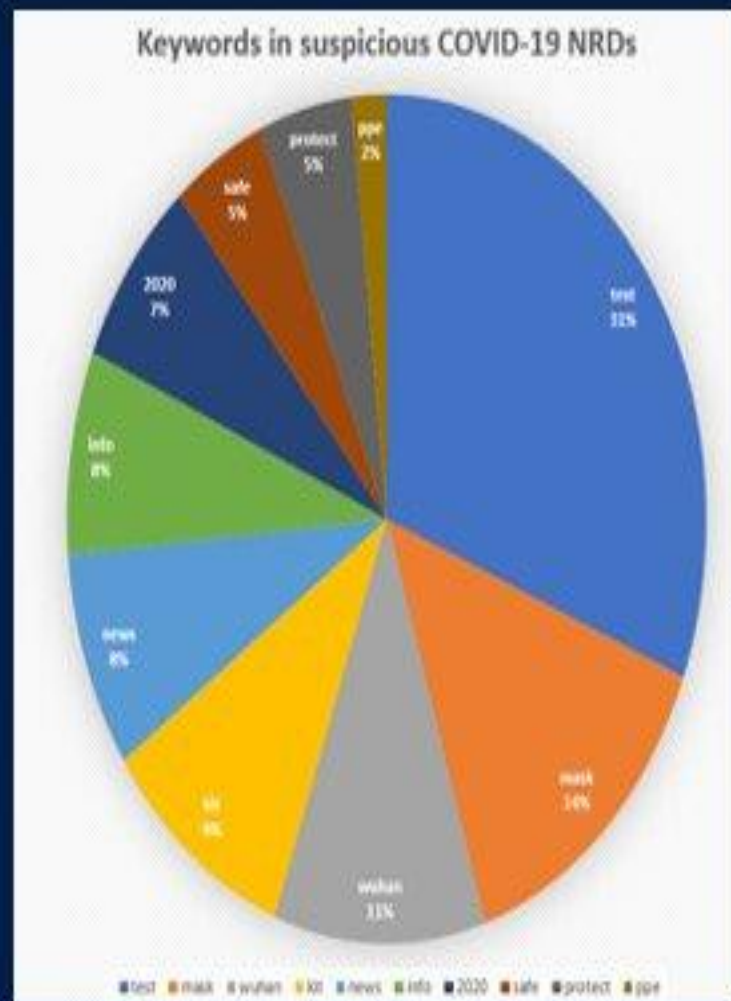
30,000% increase in phishing, websites and malware targeting remote users



COVID-19 Themed threats

COVID-19-Themed Newly Registered Domains

Over 130K Suspicious Newly Registered Domains (NRDs)



SUSPICIOUS NEWLY REGISTERED DOMAINS

survivecoronavirus[.]org

vaccine-coronavirus[.]com

coronavirus[.]cc

bestcoronavirusprotect[.]tk

coronavirusupdate[.]tk

“The IC3 was receiving between 3,000 and 4,000 cybersecurity complaints each day, a major jump from prior to the COVID-19 pandemic when about 1,000 complaints were received daily.”

Tonya Ugoretz

the deputy assistant director of the FBI's Cyber Division

April 16, 2020

“Since the beginning of the year, the FTC has received **more than 7,800 coronavirus-related reports** from consumers, **double what they were about a week ago.**”

Federal Trade Commission, USA

March 31, 2020

“According to the study of Kaspersky Lab, at the beginning of 2020, the number of attacks on Russians through scam resources increased 10 times to 15 million, and the number of such pages doubled to 10 thousand. The rapid increase is associated with the spread of the coronavirus.”

E-Hacking News

May 10, 2020

“Every day, Gmail blocks more than 100 million phishing emails.

During the last week, we saw **18 million daily malware and phishing emails related to COVID-19.**

This is in addition to more than **240 million COVID-related daily spam messages.**”

Google Cloud

May 10, 2020

FEAR

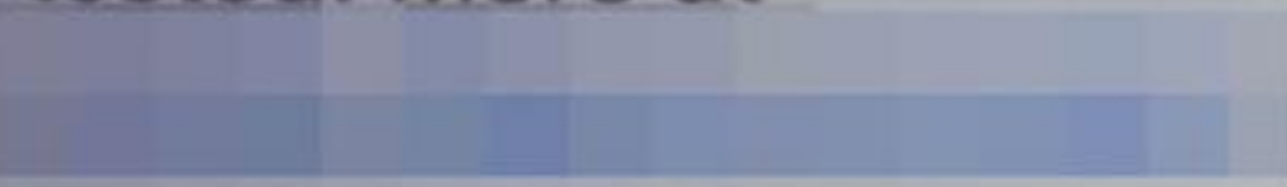
UNCERTAiNTY

DOUBT



Text Message
Today 3:45 PM

Someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at





Greater Manchester Police ✓

@gmpolice



#ScamAlert | There's a scam circulating that states the recipient has breached regulations and that a fine will be sent in the post.

This is a scam and if you receive a message like this please report to ActionFraud online [➡ crowd.in/faXNw1](https://crowd.in/faXNw1)



iMessage
Today 2:44 pm

GOV.UK CORONAVIRUS ALERT
You have been fined £3,550.73 for leaving your property without reason

♥ 113 5:58 PM - Mar 25, 2020

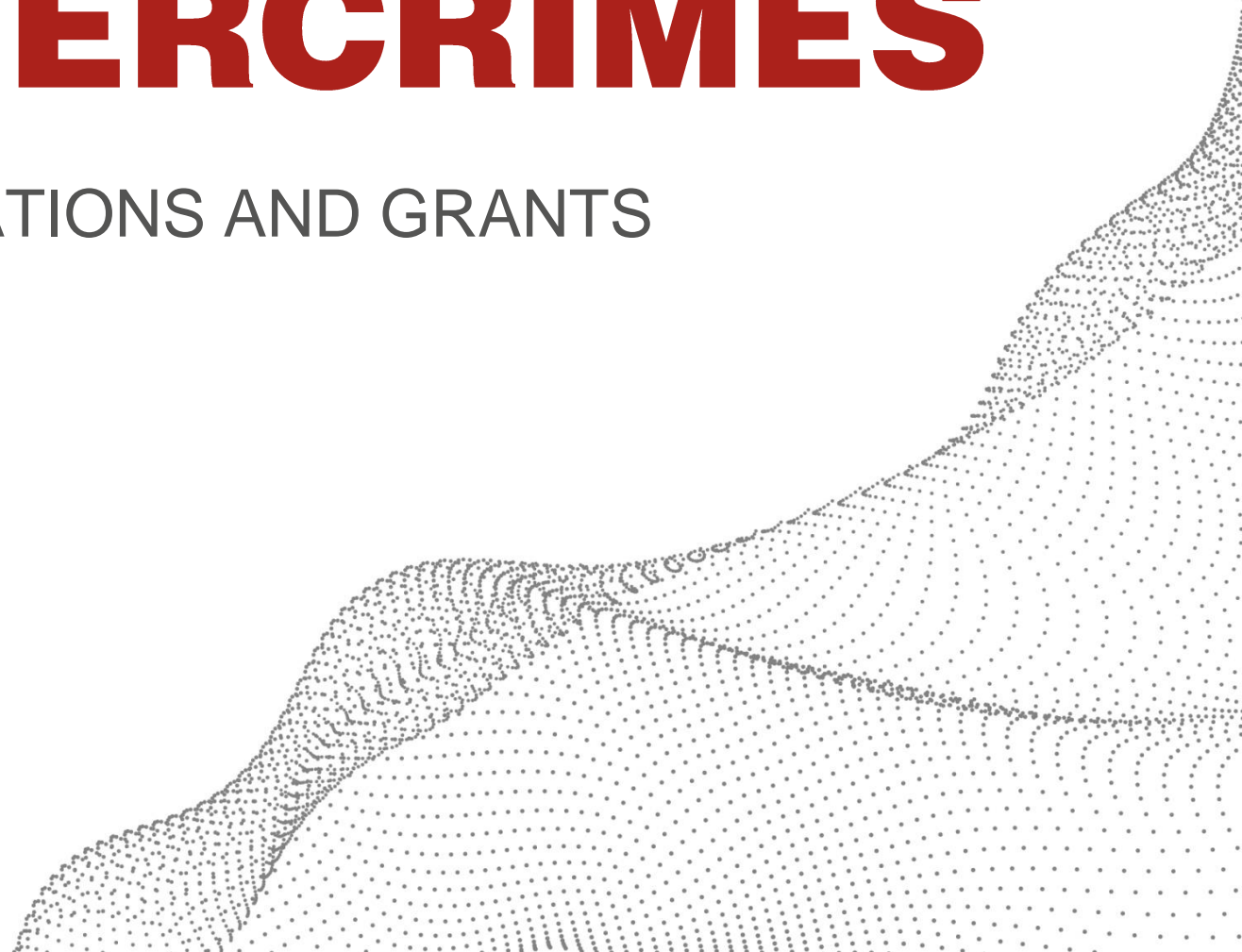


💬 227 people are talking about this



CYBERCRIMES

FAKE DONATIONS AND GRANTS



COVID-19 FUNDING

FEDERAL GOVERNMENT

\$1.102B

COMBAT CORONAVIRUS
COVID-19
RESPONSE FUND



COVID 19 FEDERAL GOVERNMENT GRANTS

The Federal Government has ordered weekly the payment of #8500 to all citizen above the age of 18 years

To receive your share of the grant, fill the form below with your correct details.

and then go to the next step.

Provide your Full Name



Provide Residential address



Phone Number



Email Address



SELECT YOUR BANK

COVID-19 FUNDING

FEDERAL GOVERNMENT

\$1.102B

COMBAT CORONAVIRUS
COVID-19
RESPONSE FUND



COVID 19 FEDERAL GOVERNMENT GRANTS

CONGRATULATIONS !!!

You Are on This Page Because You Are Eligible

For The #8500 Covid19 Federal Government Grants

To Make Sure Every Eligible Citizen gets His/Her Own Share Of The Grant.

You need to share with atleast 9 whatsapp friends or groups

Please don't be Selfish, Make Sure This Message Reaches All your Family and Friends

[Share on Whatsapp](#)

Final Step

224 ONLINE

CORONA-VIRUS DONATION Σ Spam x



meeting@nitrado.net

to Recipients ▾

09:53 (3 hours ago)



This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments or replying with personal information.

Looks safe



Hello,

I'm STEFANO PESSINA.. I'm Italian-Monegasque billionaire businessman and the vice chairman, chief executive officer (CEO), and the largest single shareholder of Walgreens Boots Alliance.. Due to this current situation (Corona Virus) that's spreading all over the world, I my self and other 19 Italian Billionaires Donate More Than \$45 Million to Fight Coronavirus In Italy... I also pledged to give away \$1,500,000.00 to Individuals, Churches and orphanage ETC... I have decided to donate 1,500,000.00USD to you because your email address was among the lucky winners.. If you are interested in my donation, do contact me for more info..

You can also read more about me via the link below

https://en.wikipedia.org/wiki/Stefano_Pessina

Warm Regard
Vice chairman and CEO,
Walgreens Boots Alliance.
Stefano Pessina

--

This email has been checked for viruses by Avast antivirus software.

<https://www.avast.com/antivirus>

CYBERCRIMES

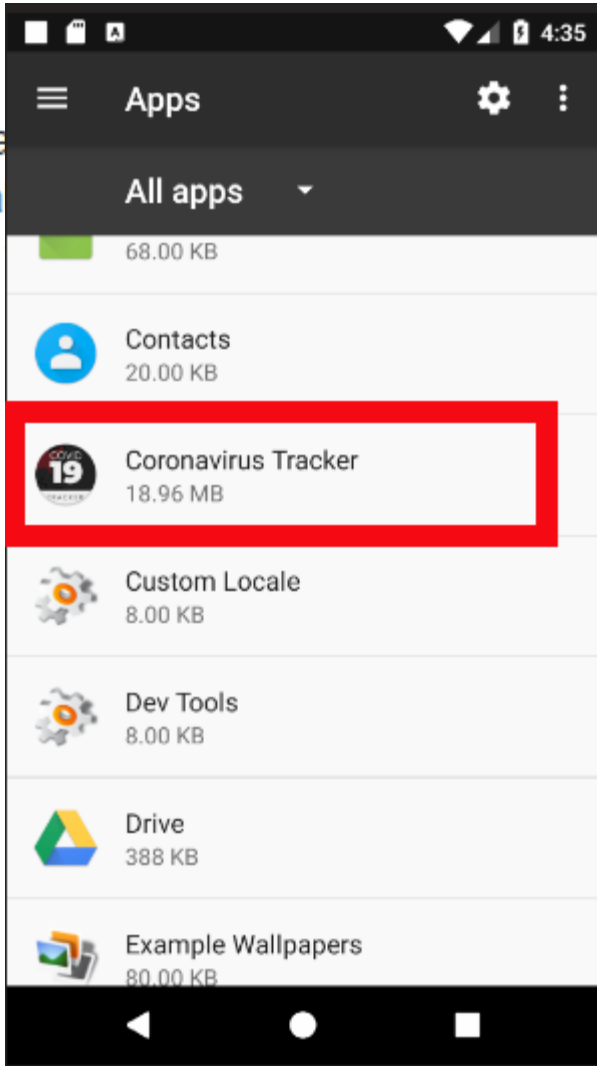
FAKE HEALTHCARE ALERTS AND PLATFORMS



CovidLock: Android Ransomware Walkthrough and Unlocking Routine

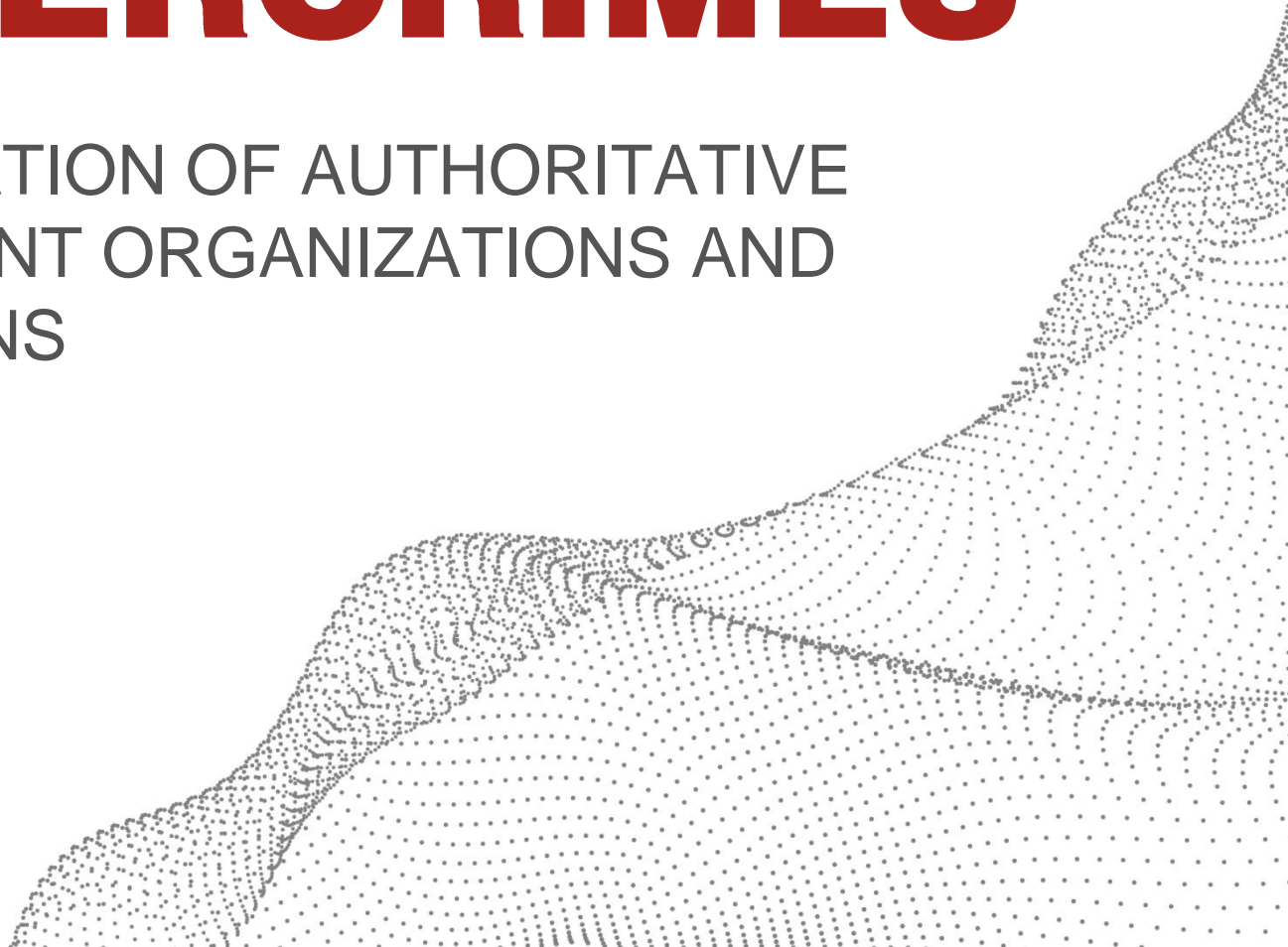
As the coronavirus has been declared a pandemic, bad actors are certainly going to take advantage of the uncertainty around it to attack a large number of online users.

The Zscaler ThreatLabZ team recently came across a URL named `hxxp://coronavirusapp[.]site/mobile.html`, which portrays itself as an Android app that tracks the coronavirus spread across the globe. In reality, it is a ransomware, which locks out the victim and asks for ransom to unlock.



CYBERCRIMES

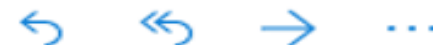
IMPERSONATION OF AUTHORITATIVE
GOVERNMENT ORGANIZATIONS AND
INSTITUTIONS



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO

World Health Organization



World Health
Organization

Dear Sir,

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

Click on the button below to download

Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

“There has been a big increase in targeting of the WHO and other cybersecurity incidents, There are no hard numbers, but such compromise attempts against us and the use of (WHO) impersonations to target others have more than doubled.”

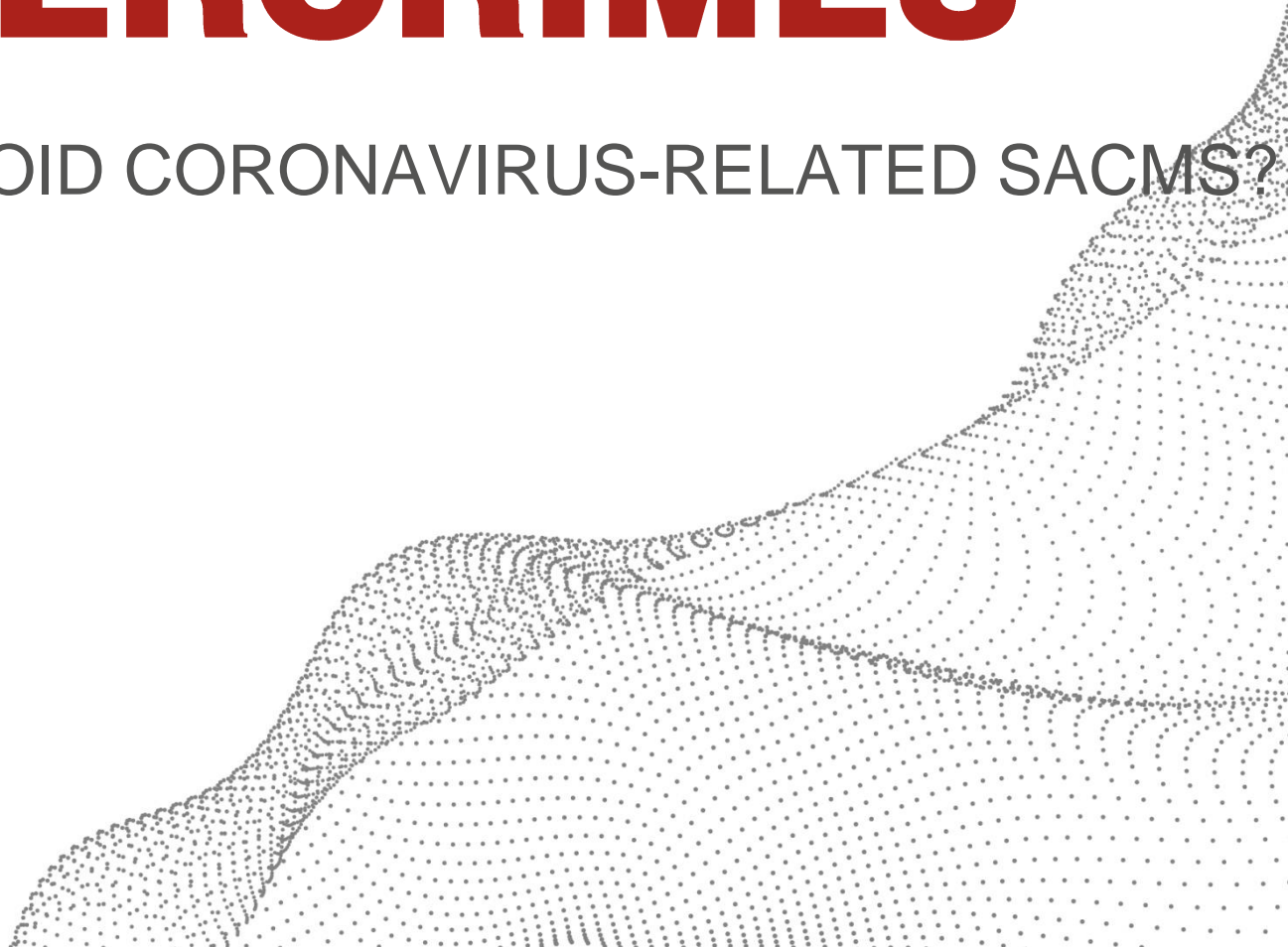
Flavio Aggio

WHO Chief Information Security Officer

March 23, 2020

CYBERCRIMES

HOW TO AVOID CORONAVIRUS-RELATED SACMS?



Beware of criminals pretending to be WHO

Hackers and cyber scammers are taking advantage of the coronavirus disease (COVID-19) pandemic by sending fraudulent email and WhatsApp messages that attempt to trick you into clicking on malicious links or opening attachments.

These actions can reveal your user name and password, which can be used to steal money or sensitive information.

If you are contacted by a person or organization that appears to be WHO, verify their authenticity before responding.

The World Health Organization will:

- **never** ask for your username or password to access safety information
- **never** email attachments you didn't ask for
- **never** ask you to visit a link outside of www.who.int
- **never** charge money to apply for a job, register for a conference, or reserve a hotel
- **never** conduct lotteries or offer prizes, grants, certificates or funding through email.

The only call for donations WHO has issued is the COVID-19 Solidarity Response Fund, which is linked to below. Any other appeal for funding or donations that appears to be from WHO is a scam.

- [COVID-19 Solidarity Response Fund](#)

Beware that criminals use email, websites, phone calls, text messages, and even fax messages for their scams.

You can verify if communication is legit by contacting WHO directly.

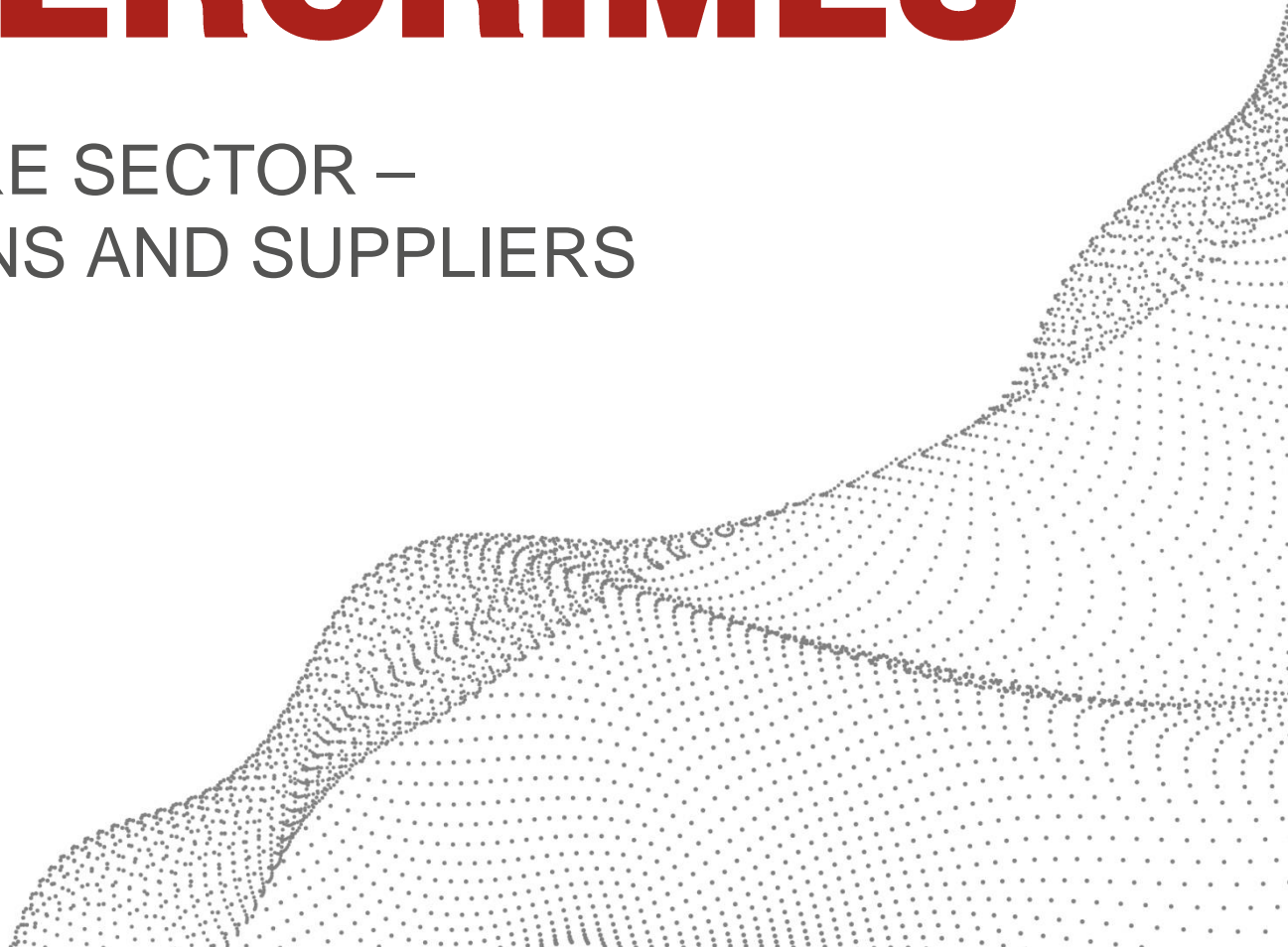
- [Contact WHO](#)
- [Report a scam](#)



World Health Organization

CYBERCRIMES

HEALTHCARE SECTOR –
INSTITUTIONS AND SUPPLIERS



Hackers hit Europe's largest healthcare provider with Snake ransomware

MAY 8TH, 2020

DEEBA AHMED

CYBER ATTACKS, CYBER CRIME

0 COMMENTS

```
Decrypt-Your-Files.txt - Notepad2
File Edit View Settings 2
-----
1 |
2 |
3 | what happened to your files?
4 |
5 |-----
6 |
7 | We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more -
8 |
9 | all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry!
10 |
11 | You can still get those files back and be up and running again in no time.
12 |
13 |-----
14 |
15 |
16 | How to contact us to get your files back?
17 |
18 |-----
19 |
20 | The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network.
21 |
22 | Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with
23 |
24 | better cyber security in mind. If you are interested in purchasing the decryption tool contact us at [REDACTED]
25 |
26 |-----
27 |
28 |
29 | How can you be certain we have the decryption tool?
30 |
31 |-----
32 |
33 | In your mail to us attach up to 3 non critical files (up to 3MB, no databases or spreadsheets).
34 |
35 | We will send them back to you decrypted.
36 |
37 |-----
38 |
39 | what happens if you dont contact us within 48 hours or refuse payment?
40 |
41 |-----
42 |
43 | We publish sensitve databases and documents we collected from your network.
44 |
45 |-----
```

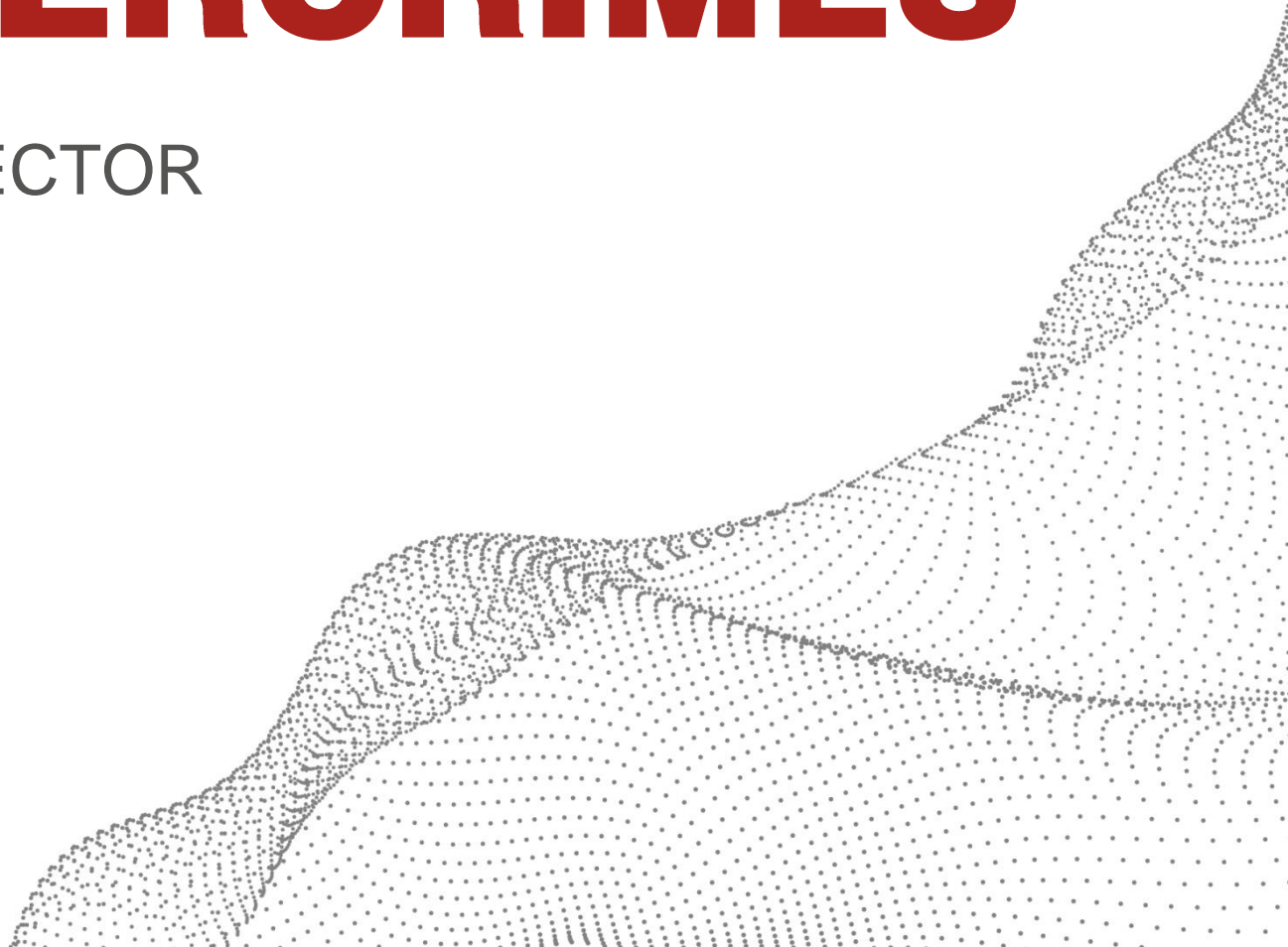
“The healthcare industry is the most targeted industry when it comes to COVID-19 related attacks, with **over 20% of campaigns targeting healthcare organizations.**”

VERINT



CYBERCRIMES

BANKING SECTOR



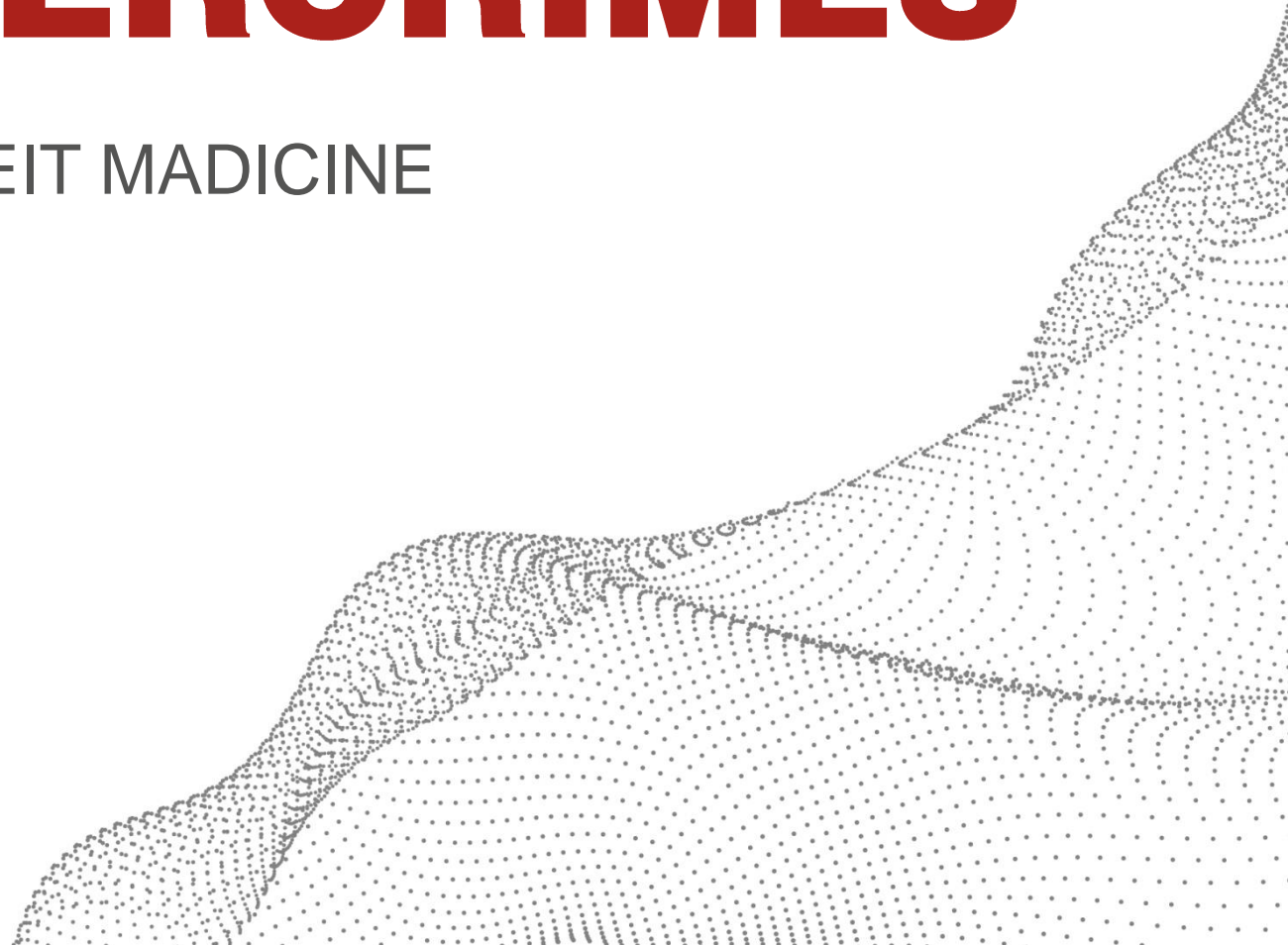
“Attacks on Banks Spike 238% ,
Ransomware attacks against the
financial sector increased nine-fold from
from the beginning of February to the end of
April 2020.

27% of attacks so far this year have
targeted either the healthcare or financial
sectors.”

VMware Carbon Black

CYBERCRIMES

COUNTERFEIT MADICINE

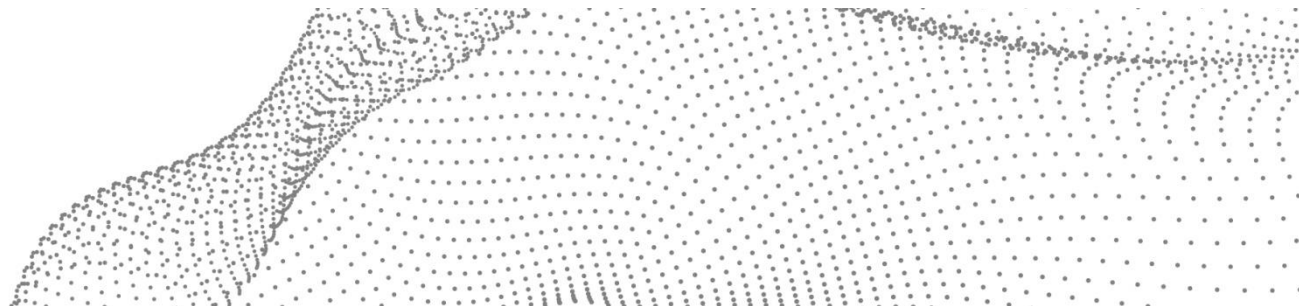


OPERATION PANGEA X



The operation in numbers

- › 121 arrests;
- › €13 million in potentially dangerous pharmaceuticals seized;
- › 326 000 packages inspected;
- › 48 000 packages seized;
- › 4.4 million units of illicit pharmaceuticals seized worldwide;
- › 37 000 unauthorised and counterfeit medical devices seized (mostly surgical masks and self-testing kits for HIV and glucose monitoring);
- › 2 500 links taken down (websites, social media, online marketplaces, adverts);
- › 37 organised crime groups dismantled.



CYBERCRIMES

NATION-STATE ACTORS



Gilead Sciences Targeted By Hackers Linked To Iran: Report



Sergei Klebnikov Forbes Staff

Markets

I cover breaking news, with a focus on money and markets.

Updated May 8, 2020, 05:12pm EDT

Iran and Russia launch cyber attacks on universities desperately searching for COVID cure

STATE-SPONSORED computer hackers from Russia and Iran have launched cyber-attacks on British research institutions fighting COVID-19, it has emerged.

By **SIMON OSBORNE**

PUBLISHED: 10:49, Sun, May 3, 2020 | UPDATED: 11:27, Sun, May 3, 2020

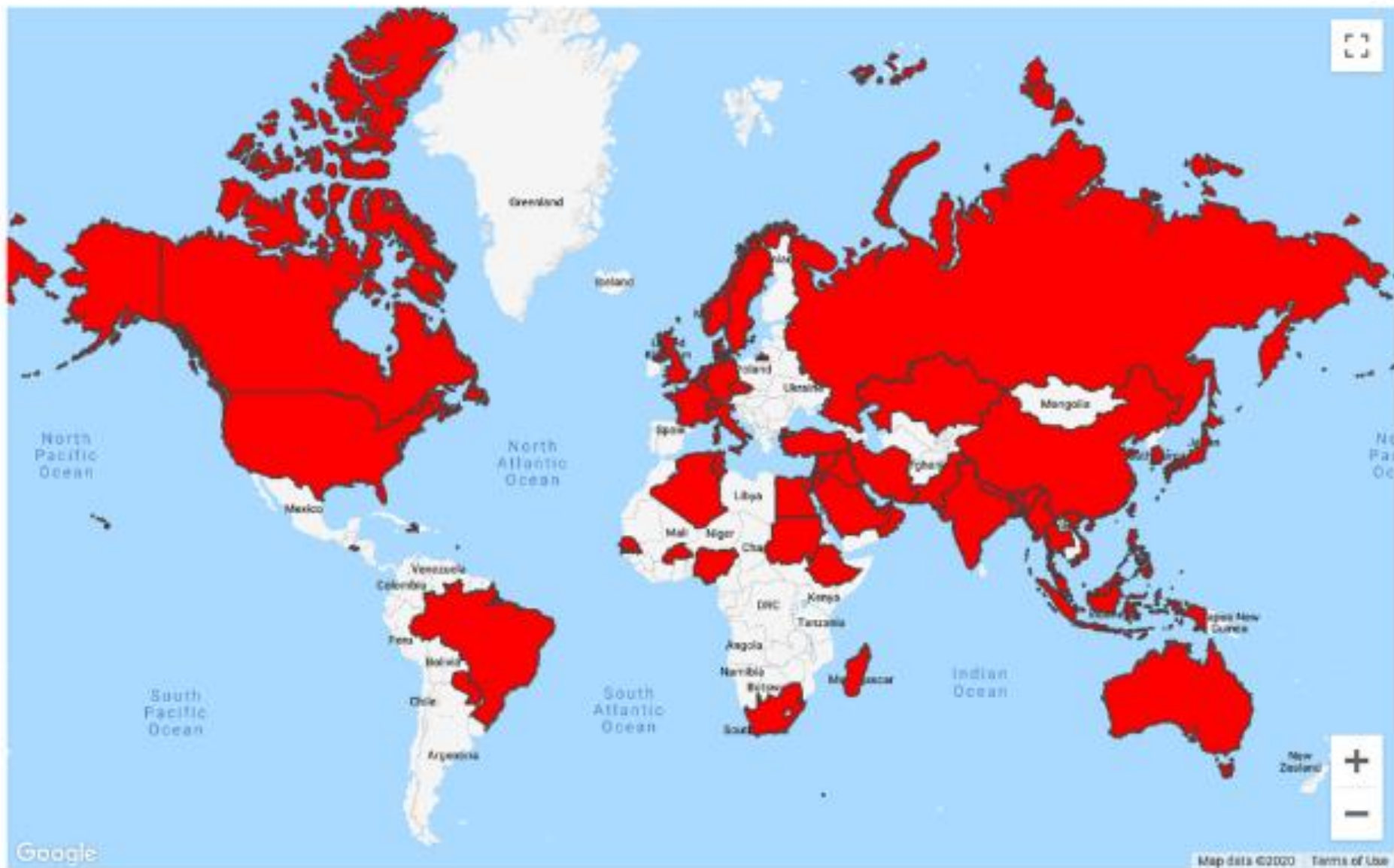
Hostile states trying to steal coronavirus research, says UK agency

Experts say Russia, Iran and China likely to be behind cyber-attacks on universities

North Korean hackers suspected of targeting vaccine maker AstraZeneca in cyberattack, Reuters reports

By Nada Bashir, Chris Liakos, [Yoonjung Seo](#), [Sophie Jeong](#) and Angus Watson, CNN

🕒 Updated 1548 GMT (2348 HKT) November 27, 2020



Location of users targeted by government-backed COVID-19 related attacks

FAKE NEWS

FAKE DONATIONS



In [#Turkey](#), people have started to leave food packets on the road for the poor and the needy who cannot earn due to [#COVID-19](#) lockdown.
Love you [#Turks](#) for representing us.

• MISLEADING





Benjamin Strick
@BenDoBrown



Disinformation on [#coronavirus](#) is rife at the moment. Here is one example. It's a viral video racking up more than 10mill views of an allegedly good deed during the [#CoronavirusLockdown](#). Actually, it's support packages for earthquake victims in January. With [@Shayan86](#) & [@_kRaay](#).



♡ 71 8:22 PM - Mar 24, 2020



💬 67 people are talking about this



FAKE NEWS

CONSPIRACIES



Beautiful message from Bill Gates

What is the Corona/ Covid-19 Virus Really Teaching us?*

I'm a strong believer that there is a spiritual purpose behind everything that happens, whether that is what we perceive as being good or being bad.

As I meditate upon this, I want to share with you what I feel the Corona/ Covid-19 virus is really doing to us:

1) It is reminding us that we are all equal, regardless of our culture, religion, occupation, financial situation or how famous we are. This disease treats us as we should to. If you don't believe me, just ask Tom

• **FAKE**

2) It is reminding us that we are all connected and something that affects one person has an effect on another. It is reminding us that the false borders that we have put up have little value as this virus does not need a passport. It is reminding us, by oppressing us for a short time, of those in this world whose whole life is spent in oppression.

3) It is reminding us of how precious our health is and how we have moved to neglect it through eating nutrient poor manufactured food and drinking water that is contaminated with chemicals upon chemicals. If we don't look after our health, we will, of course, get sick.

4) It is reminding us of the shortness of life and of what is most important for us to do, which is to help each other, especially those who are old or sick. Our purpose is not to buy toilet roll.

- **NO EVIDENCE**

Tonight from 11.30pm nobody should be on the street. Doors and windows should remain closed as helicopters spray disinfectants into the air to eradicate the coronavirus. Please spread this information to all your contacts

Conspiracy theorists are falsely claiming that the coronavirus pandemic is an elaborate hoax

April 23, 2020 1.36am AEST

and not touching your face.

If you feel sick, PLEASE DO NOT VISIT.



FAKE NEWS

FAKE NEWS AND MINORITIES





04.08.2020

HUNGARY

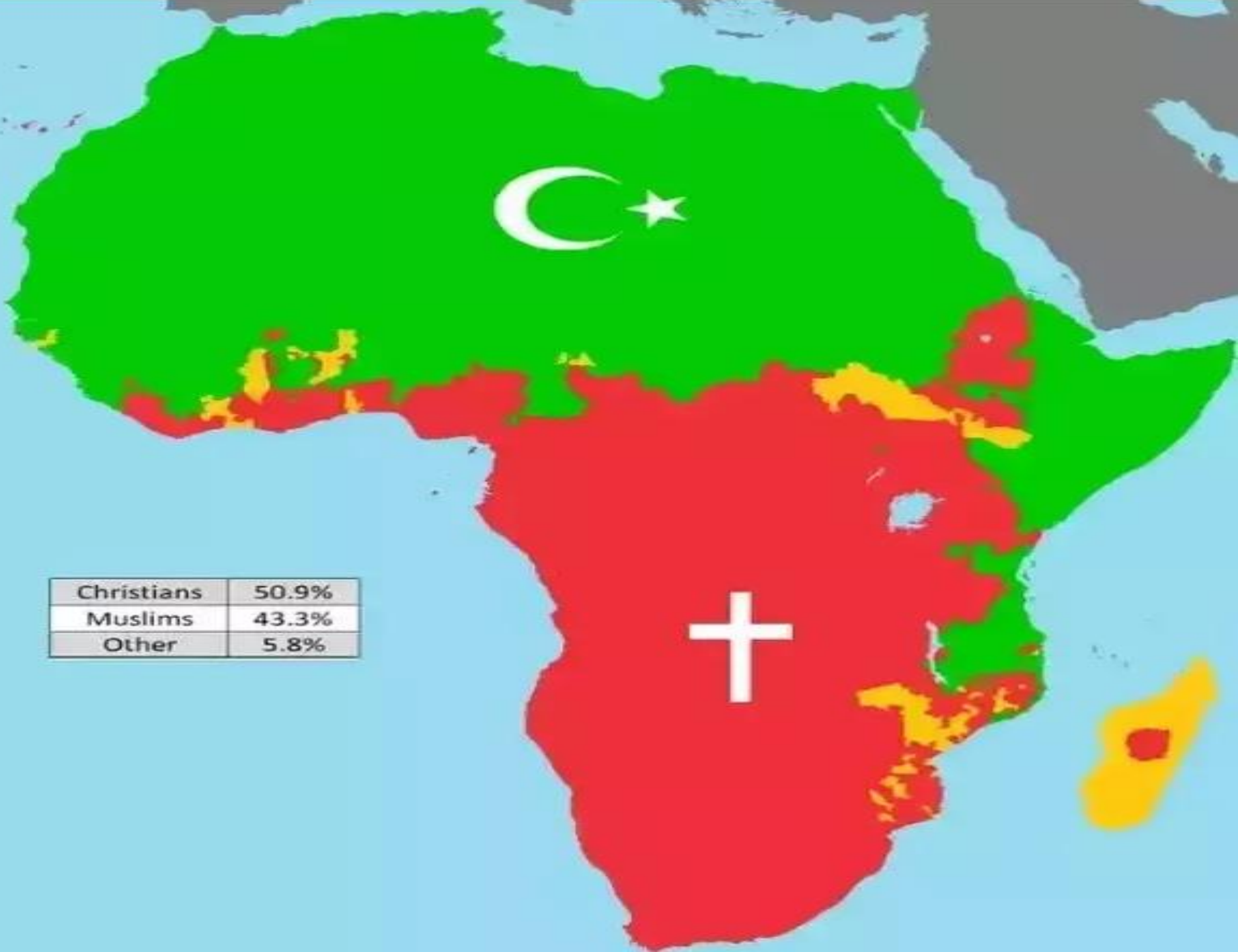
LAW / POLICIN

Viktor Orbán is Using the Coronavirus Emergency to Crush Minorities



Asia & Pacific

As the world looks for coronavirus scapegoats, Muslims are blamed in India





WORLD NEWS

Coronavirus conspiracy theories putting Christian minorities at risk

Mon 20 Apr 2020 by Premier Journalist




Russia and China push 'fake news' aimed at weakening Europe: report

EU officials claim both Moscow and Beijing continue to peddle disinformation on social media whose aim is to undermine the European Union and its partners.

By **MARK SCOTT** | 4/1/20, 6:01 AM CET | Updated 4/1/20, 8:57 PM CET

Ростовская

THE "CRUCIFIED BOY" – UKRAINE, JULY 2014



and they nailed him like Jesus
to the message board.

WWW.1TV.RU

Ridiculous lie on Russian TV: a child was crucified in Ukraine.

"Crucified Boy" ([Russian](#): Распятый мальчик, Raspyaty malchik) was the news episode that was officially titled "A refugee from [Sloviansk](#) recalls how a little son and a wife of a [militiaman](#) were executed in front of her" and was shown on the state-owned [Channel One Russia](#) during the [War in Donbass](#), on July 12, 2014. It contained information about an unconfirmed (or faked) case of the public [crucifixion](#) of a three-year-old boy by [Ukrainian soldiers](#) at the Lenin Square in Sloviansk. This episode was later widely used as **an example of "[disinformation](#)" or "lies", that "became the standard" for modern [mass media](#)**, especially Russian official ones. **In Russian mass culture the episode - this "[good piece of propaganda](#)" - became a "[synonymous for journalist fake](#)".** The spread of the news about "crucified boy" was later used for [statistical analysis](#) of the expansion of fake information in modern [social networks](#) and [search engines](#).^{[5][6]}

THE "LISA CASE" - GERMANY, JANUARY 2016

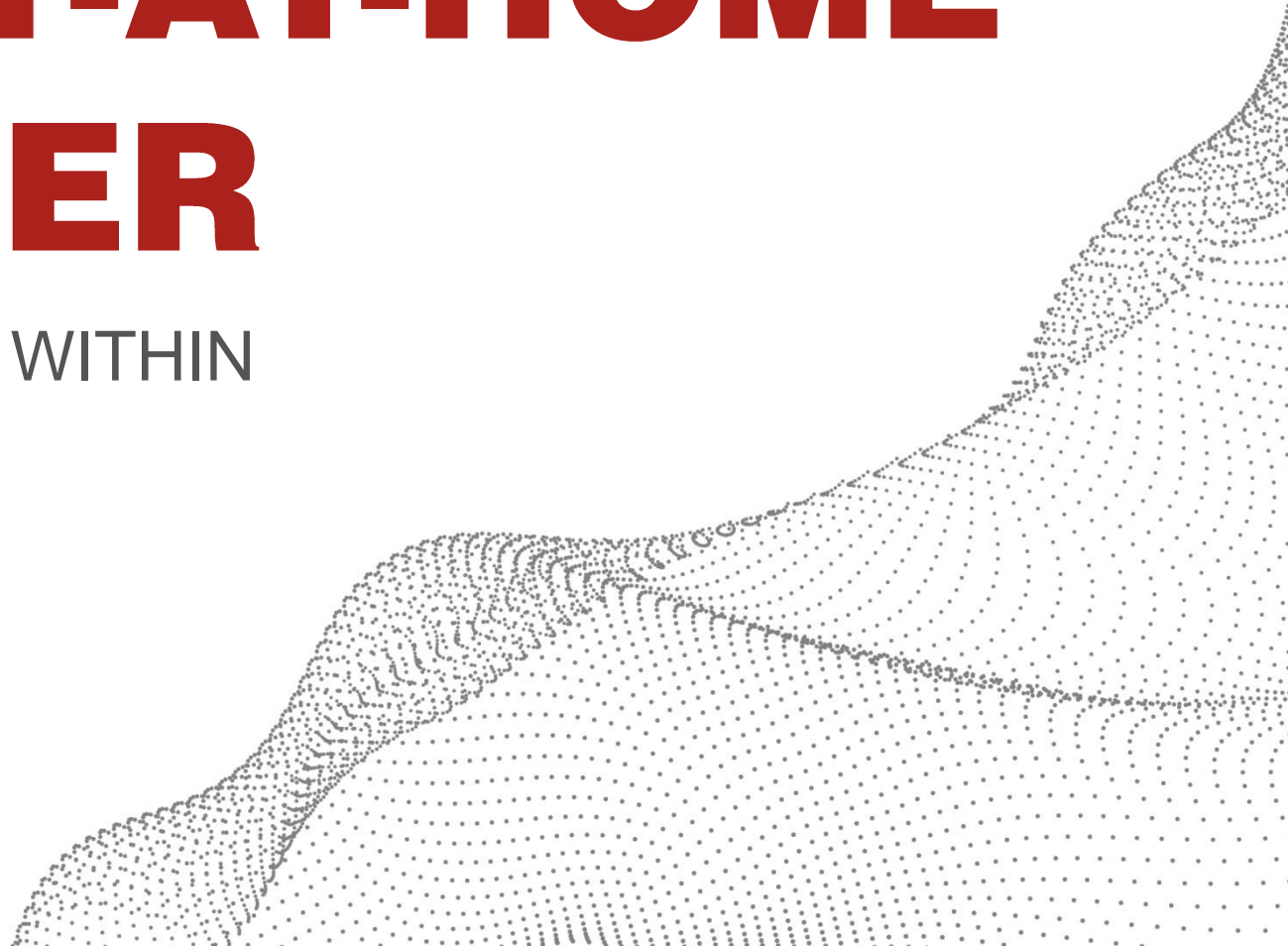


The "Lisa case": Germany as a target of Russian disinformation

The media storm surrounding a fake story about a Russian-German girl, who had reportedly been raped by Arab migrants, was a wake up call for German political elites earlier this year. For the first time, they clearly saw the links between Russian domestic and foreign media campaigns against Germany and Russian politics at the highest level. The German government promptly advised the Federal Intelligence Service (BND) in coordination with the Foreign Office to check Russian sources of manipulation of German public opinion.

STAY-AT-HOME ORDER

THE ENEMY WITHIN



“We're reaching a period where everyone is somewhat uncertain.

A lot of the insider threat is driven by personal factors.”

Joseph Blankenship

Vice president and research director with Forrester

May 8, 2020

STAY-AT-HOME ORDER

WORK FROM HOME



From: shenyeh5@gmail.com
Sent on: Saturday, April 11, 2020 7:39:58 PM
To: [REDACTED]
Subject: WORK FROM HOME

Hello,

DO you live in CANADA/USA and you are laid off from work due to the recent global crisis with Covid 19? You can work from home and get paid \$5,000 monthly. email me for more details.

shenyeh5@gmail.com

Work from home!



[REDACTED]

To: [REDACTED]

Wednesday, April 29, 2020 at 4:52 PM

Dear ,

How are you feeling today? My name is [REDACTED]. I work for [REDACTED] as a Human resource (HR). We are currently recruiting people that which to work from home and likewise help us run little errands around the united states. We need a personal assistant to work for our company and do our personal chores. Our great company is now short of staff because of the current pandemic outbreak in the world which is very sad. As we have lost great staff and vital important people. This is painful and we send our sincere prayers to their families.

Furthermore, this job is open for people that are ready to earn extra income while they even maintain their full-time business. You really do not need a work experience because AS, a company we train you and make you understand the little task in your front. This is a part time job If you interested let us know by your response to this message. You will have to work from home because of the Coronavirus. And if you need to go out, our company will provide every necessary assistance you need.

Yours faithful

[REDACTED]

From: home_connect@

Date: Sat, Apr 4, 2020 at 3:08 PM

Subject: (Virtual-Lab) Stay-At-Home Connection -9435

To:

Testing our Virtual Lab Machines, Please connect from home to access our requisition platform SAP/Concur.

<http://virtual-lab.com/homeaccess>

Thanks,
IT Tech

From: [remote_access_VPN@](#)

Date: Fri, Apr 3, 2020 at 4:48 PM

Subject: (VPN) configuration secured link -2874

To:

New VPN configuration home access.

<http://portal.remoteaccess/vpnconfiguration>

Login with your email and password.

Thanks,
IT Support

STAY-AT-HOME ORDER

THE CONSEQUENCES





51%

of organizations have already seen an increase in email phishing attacks since shifting to a remote working model

 **Barracuda.**
Your journey, secured.

“51% of respondents said their workforce is not proficient or properly trained in the cyber risks associated with remote working.

46% are not confident their web applications are secure.

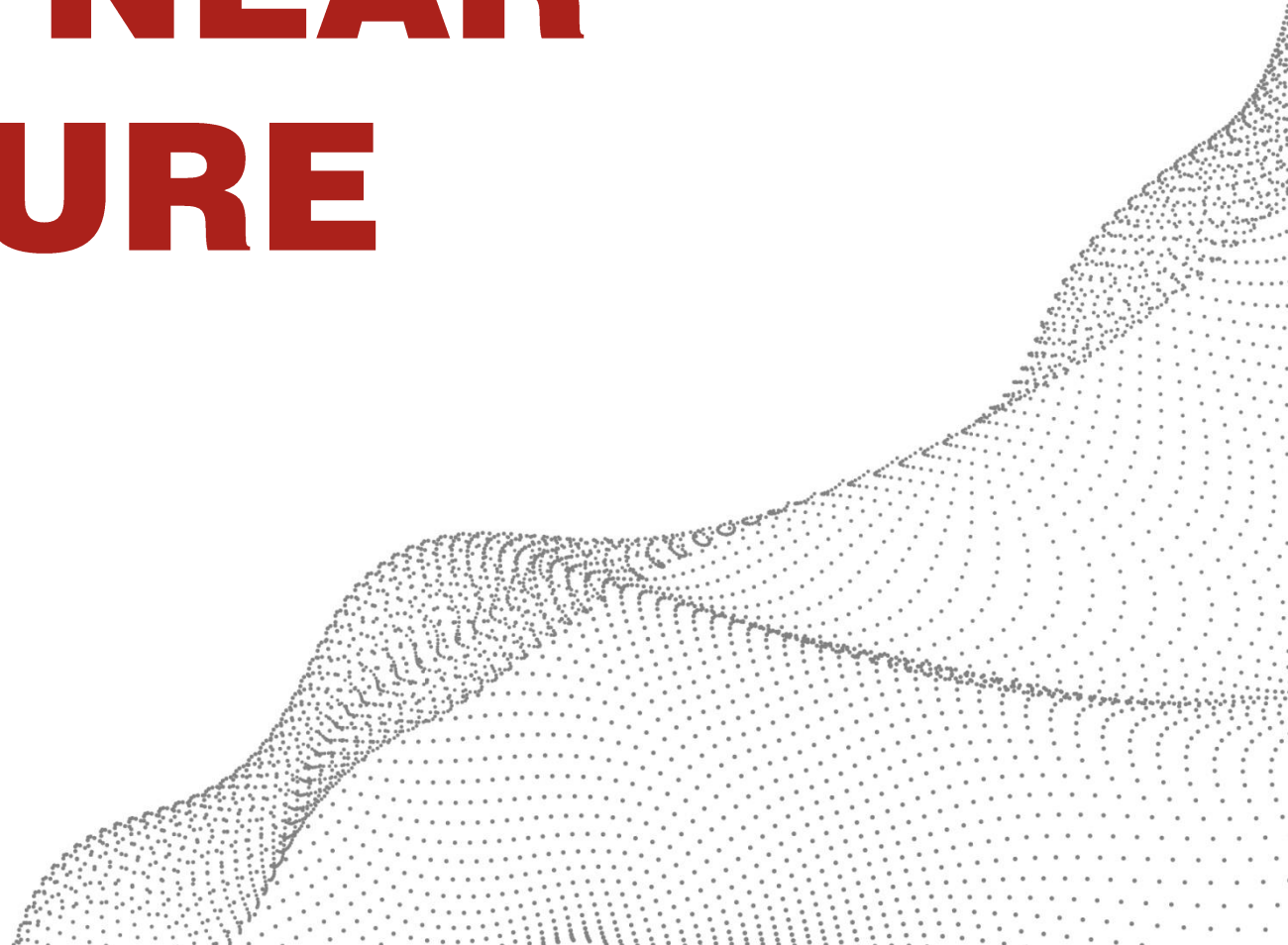
50% have allowed employees to use personal email address and personal devices to conduct company work.

40% of respondents have cut their cybersecurity budgets as a cost saving measure to help tackle the COVID-19 crisis.”

Barracuda

May 6, 2020

THE NEAR FUTURE





56%

of organizations plan to continue widespread remote working even after the COVID-19 crisis is over

“The coronavirus is laying the groundwork for a massive cyberattack. In fact, I’m on record today saying we’ll see the largest cyberattack in HISTORY within the next six months.”

Coronavirus practically guarantees “largest cyberattack ever” will soon be plastered all over the frontpages.”

Forbes

May 14, 2020

“Hundreds of millions of folks are using **personal laptops**—on **unsecured home internet connections**—to **access work files**. Many of which likely **contain confidential information and personal data**.

This is a dream come true for cyber criminals. Hackers only need to gain access through **one entry point to seize control of a whole network**. Once they're in they can steal data, secrets, and even lock you out of the network.”

Forbes

May 14, 2020

“Hackers broke into the networks of **America’s largest defense contractor, Lockheed Martin, by targeting remote workers**. If they can infiltrate this system, you best believe remote workers with little security are easy pickings.”

Forbes

May 14, 2020

Two in Five Home Workers Vulnerable to Cyber-Attacks

Two in five remote workers in the UK are vulnerable to cyber-attacks as they have not received information about how to avoid COVID-19 scams or had any video call security training. This is according to a new report by [Fasthosts](#), which looked at the additional cyber-risks businesses are facing as a result of the shift to home working this year.

The study also found that over half (54%) of remote workers are currently operating without a VPN, potentially increasing the risk of personal and company data getting compromised. Additionally, around a quarter allow others in their household look at confidential documents.

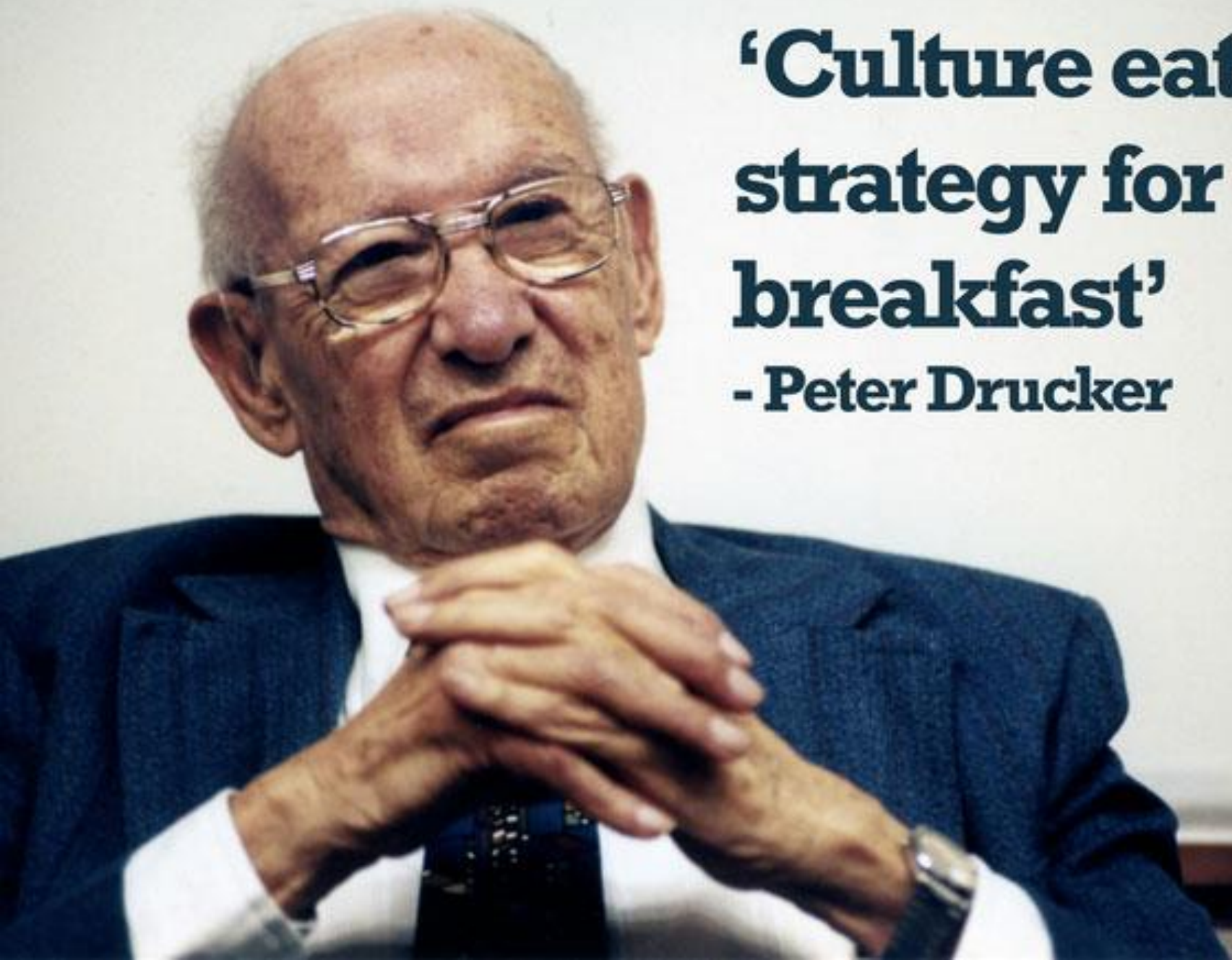
The researchers revealed that those employed in the science and pharmaceutical industry were most likely to allow other members of their household access to their work computer/laptop, while law enforcement and security staff were the biggest culprits in allowing access to confidential data and documents.

DANGER

“The crisis will end, but the threats will persist.
Protect your enterprise.”

Zscaler

April 23, 2020




**‘Culture eats
strategy for
breakfast’
- Peter Drucker**

11/16/2018
10:30 AM

95% of Organizations Have Cultural Issues Around Cybersecurity

Very few organizations have yet baked cybersecurity into their corporate DNA, research finds.



A scenic landscape at sunset. The sun is low on the horizon, casting a warm, golden glow over the scene. A dirt road curves through the landscape, and a stream flows through the foreground. The sky is filled with soft, golden light, and the overall atmosphere is peaceful and contemplative.

Security is a process,
not a product.

Bruce Schneier

“I think we are really going to see
an unprecedented wave of
cyber attacks and cyber
fraud.

And that's what we're trying to
prepare our partners and the
public for.”

United States Attorney, Scott Brady

March 18, 2020



TAL PAVEL, PHD

Founder & Director

The Institute for Cyber Policy Studies

The Institute for Cyber Policy Studies

Cybureau.org | Tal@cybureau.org | +972-525-258-985