CYBERSECURITY
EXPERTS ON YOUR SIDE

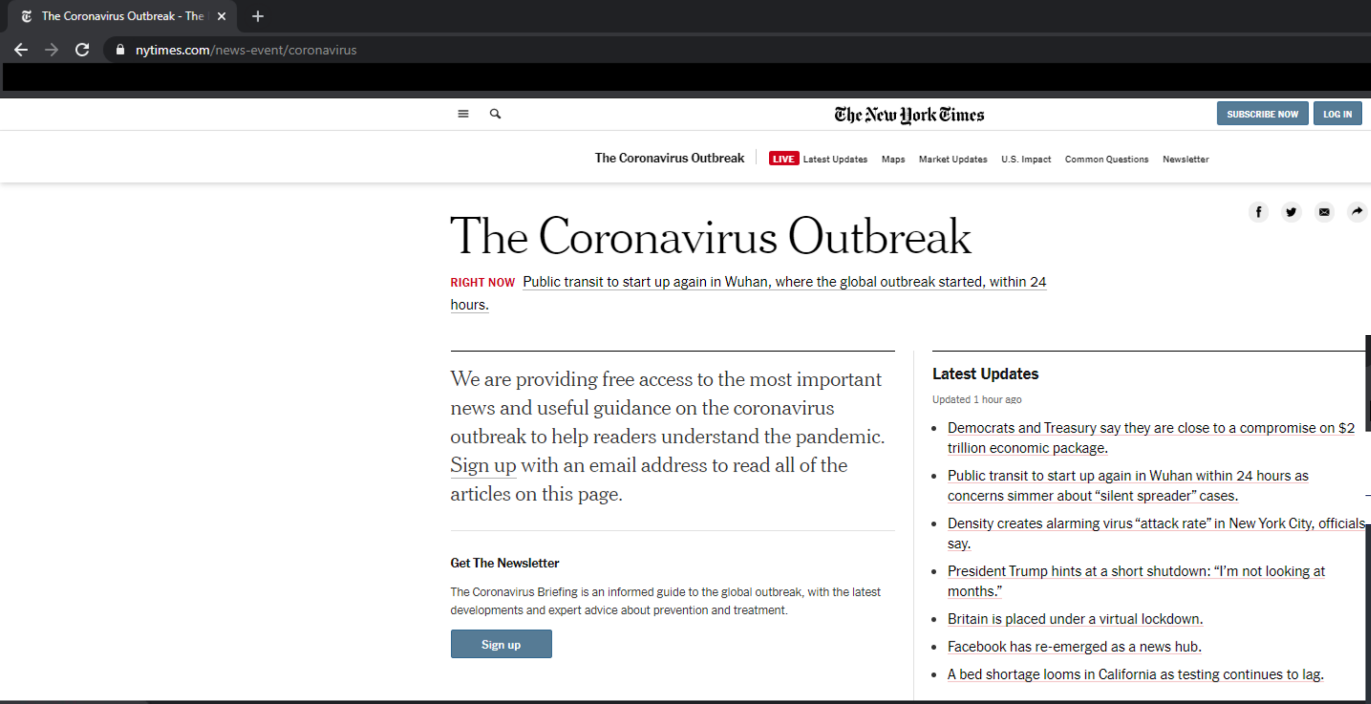
Kyberhrozby v čase pandémie aj mimo nej

Ondrej Kubovič @OndrashMachula

Ondrej Kubovič

Security Awareness Specialist

COVID-19



The Coronavirus Outbreak

RIGHT NOW Public transit to start up again in Wuhan, where the global outbreak started, within 24 hours.

We are providing free access to the most important news and useful guidance on the coronavirus outbreak to help readers understand the pandemic. Sign up with an email address to read all of the articles on this page.

Get The Newsletter

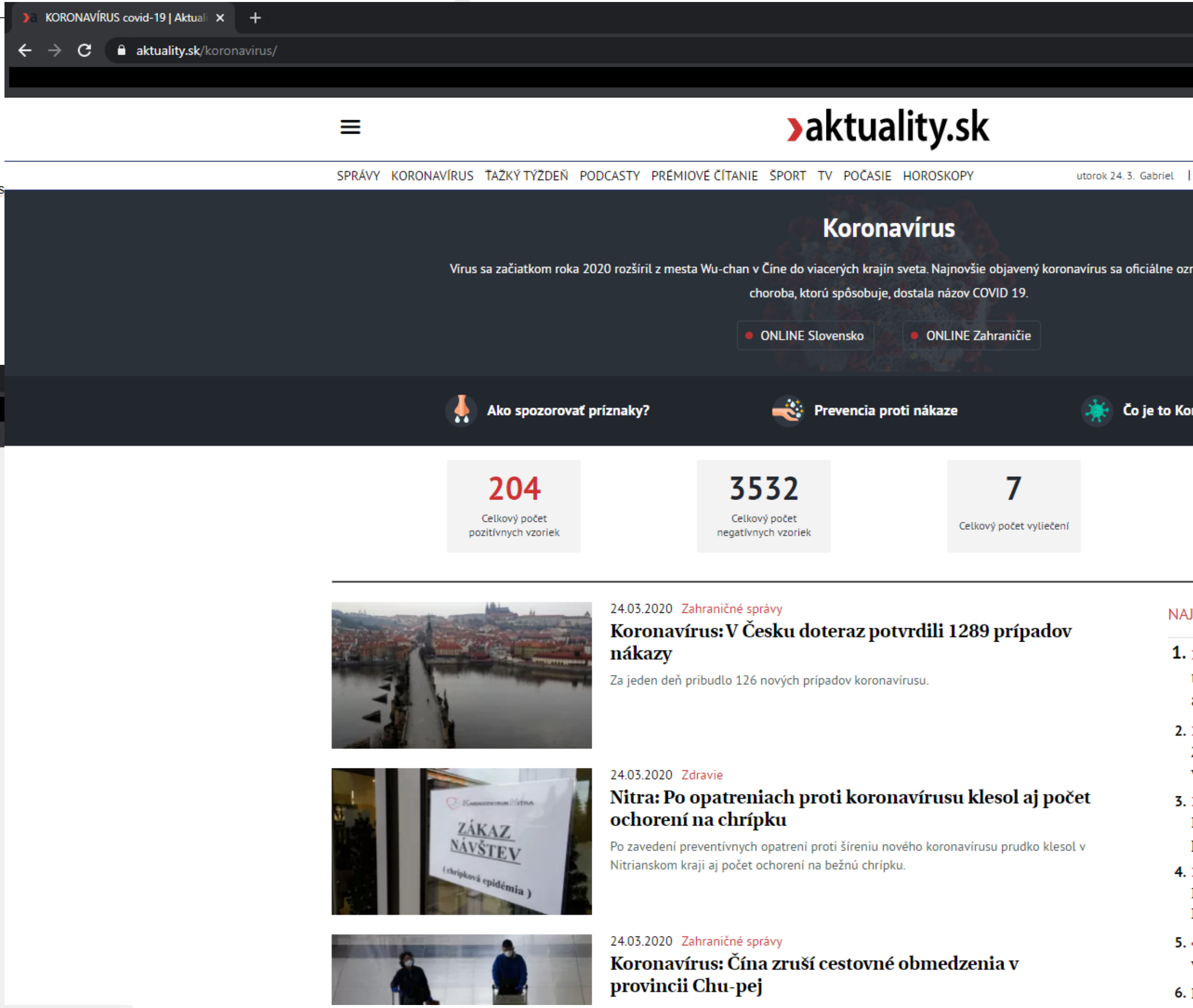
The Coronavirus Briefing is an informed guide to the global outbreak, with the latest developments and expert advice about prevention and treatment.

Sign up

Latest Updates

Updated 1 hour ago

- Democrats and Treasury say they are close to a compromise on $2 trillion economic package.
- Public transit to start up again in Wuhan within 24 hours as concerns simmer about "silent spreader" cases.
- Density creates alarming virus "attack rate" in New York City, officials say.
- President Trump hints at a short shutdown: "I'm not looking at months."
- Britain is placed under a virtual lockdown.
- Facebook has re-emerged as a news hub.
- A bed shortage looms in California as testing continues to lag.



Koronavírus

Vírus sa začiatkom roka 2020 rozšíril z mesta Wu-chan v Číne do viacerých krajín sveta. Najnovšie objavený koronavírus sa oficiálne oz choroba, ktorú spôsobuje, dostala názov COVID 19.

204	3532	7
Celkový počet pozitívnych vzoriek	Celkový počet negatívnych vzoriek	Celkový počet vyliečení

24.03.2020 Zahraničné správy

Koronavírus: V Česku doteraz potvrdili 1289 prípadov nákazy

Za jeden deň pribudlo 126 nových prípadov koronavírusu.

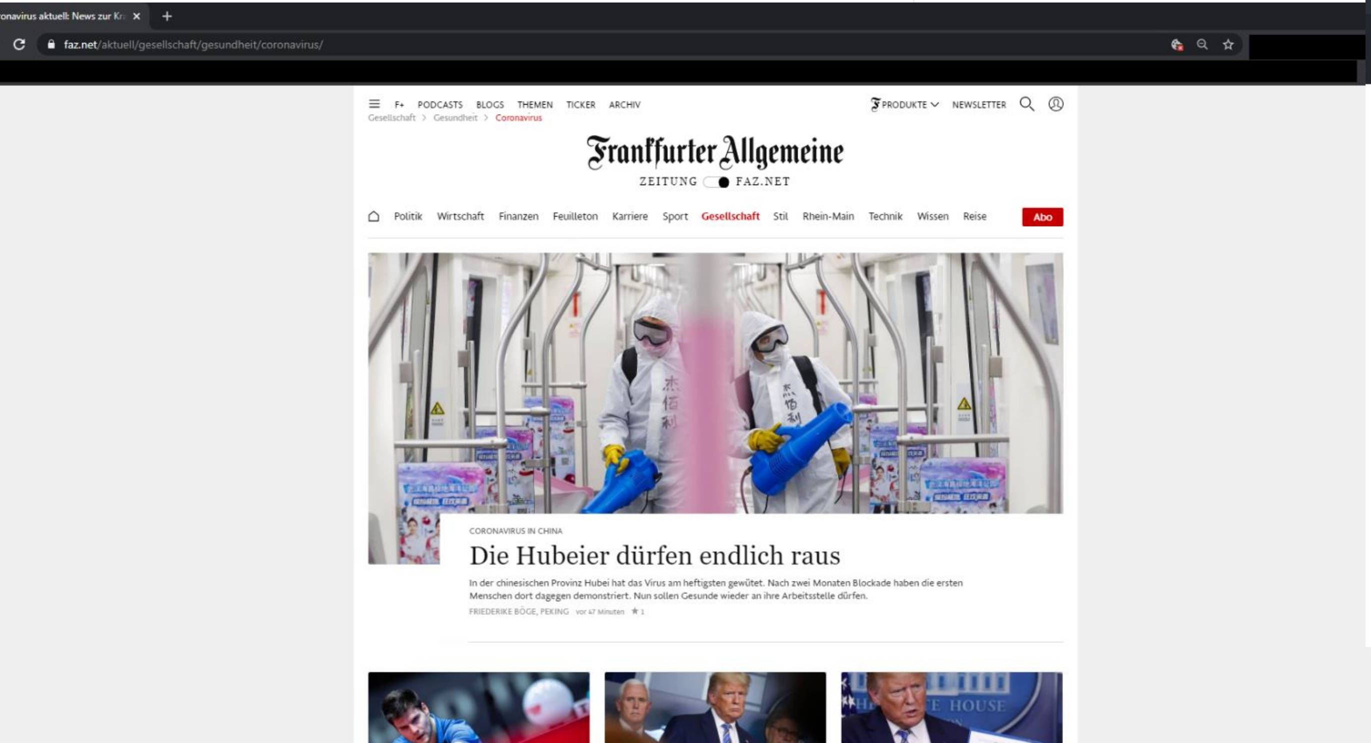
24.03.2020 Zdravie

Nitra: Po opatreniach proti koronavírusu klesol aj počet ochorení na chrípku

Po zavedení preventívnych opatrení proti šíreniu nového koronavírusu prudko klesol v Nitrianskom kraji aj počet ochorení na bežnú chrípku.

24.03.2020 Zahraničné správy

Koronavírus: Čína zruší cestovné obmedzenia v provincii Chu-pej

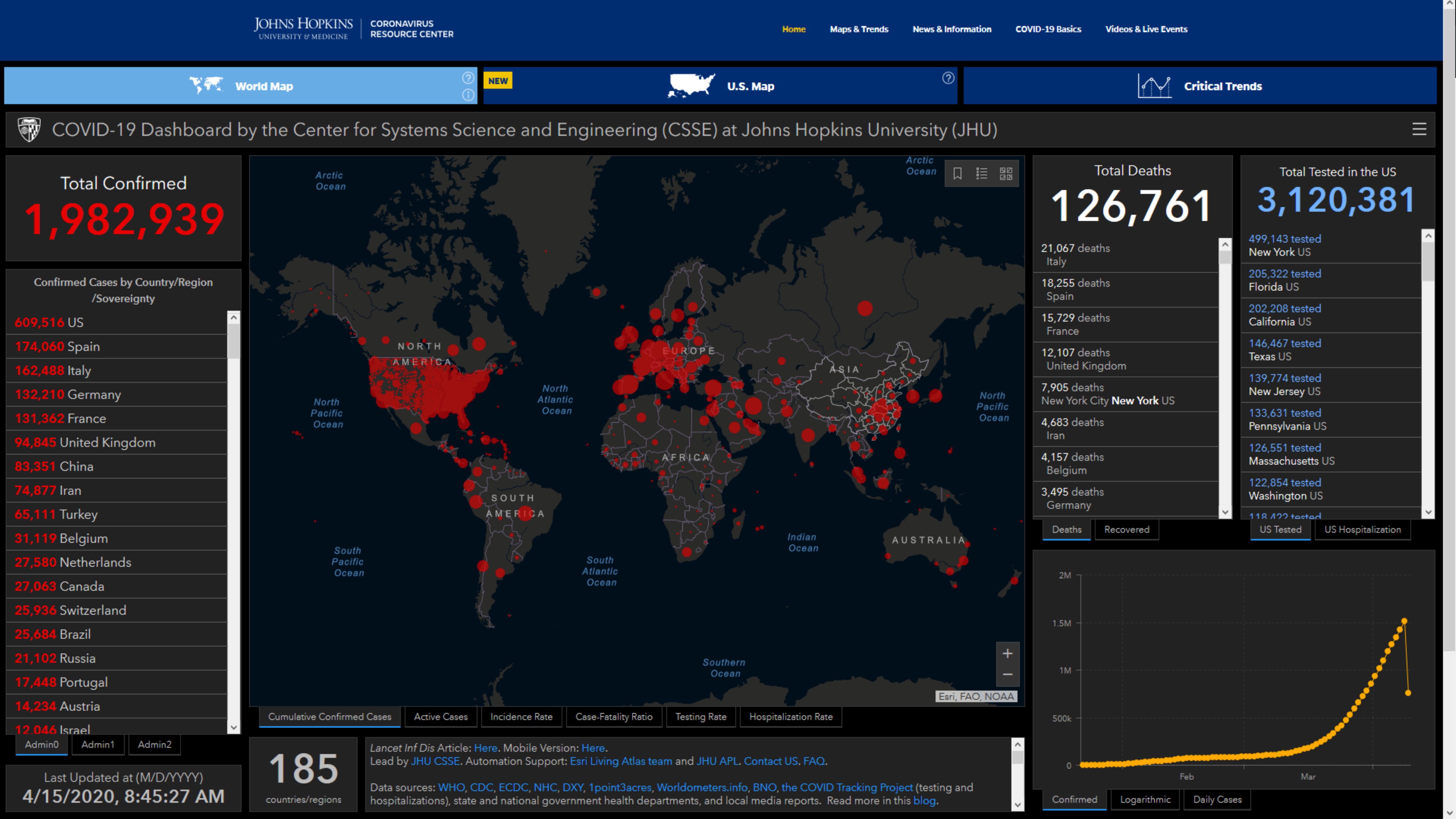


CORONAVIRUS IN CHINA

Die Hubeier dürfen endlich raus

In der chinesischen Provinz Hubei hat das Virus am heftigsten gewütet. Nach zwei Monaten Blockade haben die ersten Menschen dort dagegen demonstriert. Nun sollen Gesunde wieder an ihre Arbeitsstelle dürfen.

FRIEDERIKE BÖGE, PEKING vor 47 Minuten ★ 1



COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

Total Confirmed
1,982,939

Confirmed Cases by Country/Region /Sovereignty

609,516	US
174,060	Spain
162,488	Italy
132,210	Germany
131,362	France
94,845	United Kingdom
83,351	China
74,877	Iran
65,111	Turkey
31,119	Belgium
27,580	Netherlands
27,063	Canada
25,936	Switzerland
25,684	Brazil
21,102	Russia
17,448	Portugal
14,234	Austria
12,046	Israel

Last Updated at (M/D/YYYY)
4/15/2020, 8:45:27 AM

185
countries/regions

Lancet Inf Dis Article: Here. Mobile Version: Here.
Lead by JHU CSSE. Automation Support: Esri Living Atlas team and JHU APL. Contact US. FAQ.

Data sources: WHO, CDC, ECDC, NHC, DXY, 1point3acres, Worldometers.info, BNO, the COVID Tracking Project (testing and hospitalizations), state and national government health departments, and local media reports. Read more in this blog.

Total Deaths
126,761

21,067 deaths	Italy
18,255 deaths	Spain
15,729 deaths	France
12,107 deaths	United Kingdom
7,905 deaths	New York City **New York** US
4,683 deaths	Iran
4,157 deaths	Belgium
3,495 deaths	Germany

Total Tested in the US
3,120,381

499,143 tested	New York US
205,322 tested	Florida US
202,208 tested	California US
146,467 tested	Texas US
139,774 tested	New Jersey US
133,631 tested	Pennsylvania US
126,551 tested	Massachusetts US
122,854 tested	Washington US
118,422 tested	

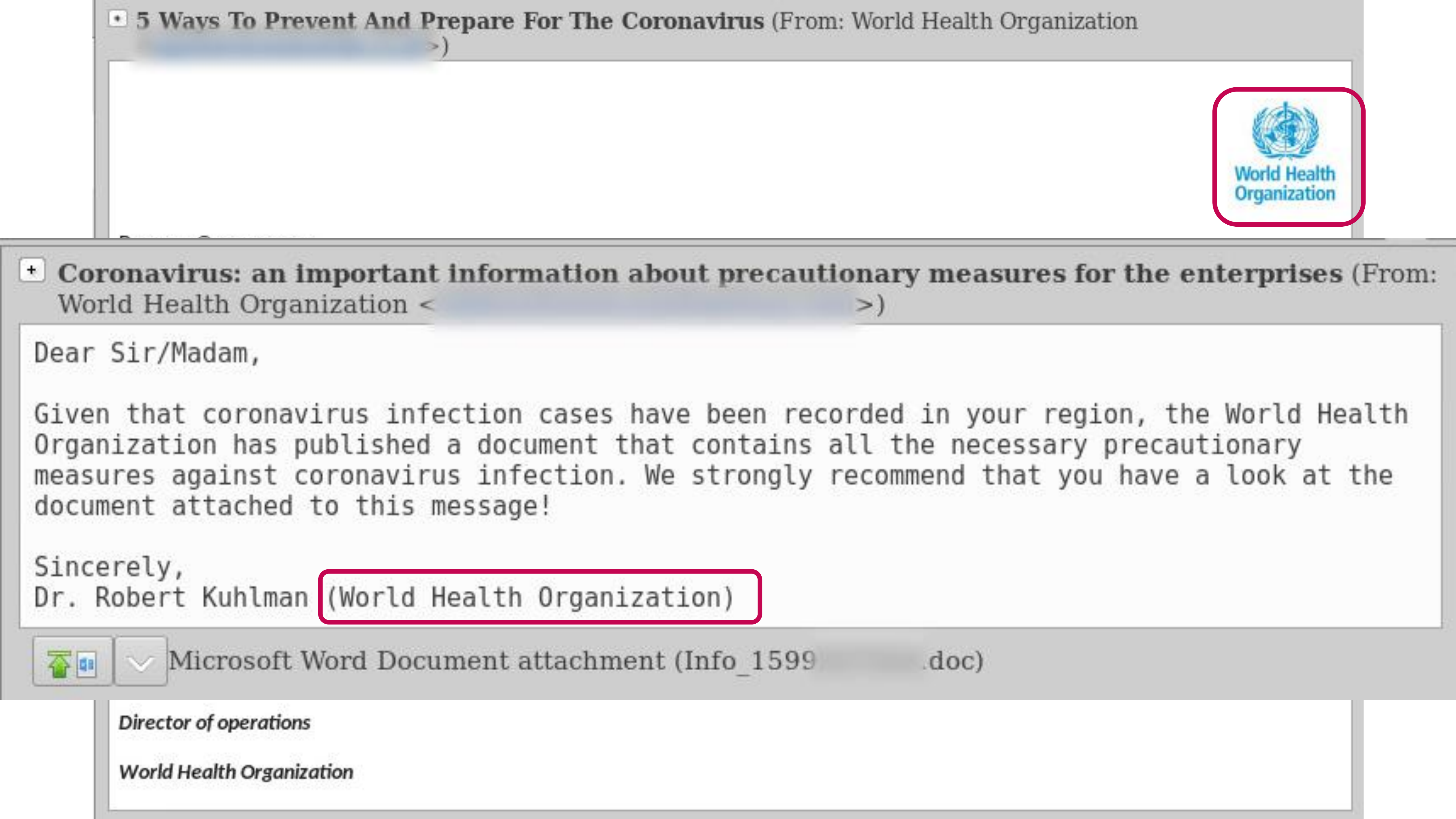
CAUTION
QUARANTINE
AREA
SmartSign.com • 800-952-1457 • S-0414

Knoppers

Scam, spam, phishing

Populárne témy COVID-19 scam kampaní

- „Nigerijský princ“
- Falošné WHO
- Zabudnuté faktúry, objednávky
- Zoznam prísad na výrobu domácej vakcíny
- Vyhrážky a vydieranie



5 Ways To Prevent And Prepare For The Coronavirus (From: World Health Organization [redacted]>)

Coronavirus: an important information about precautionary measures for the enterprises (From: World Health Organization <[redacted]>)

Dear Sir/Madam,

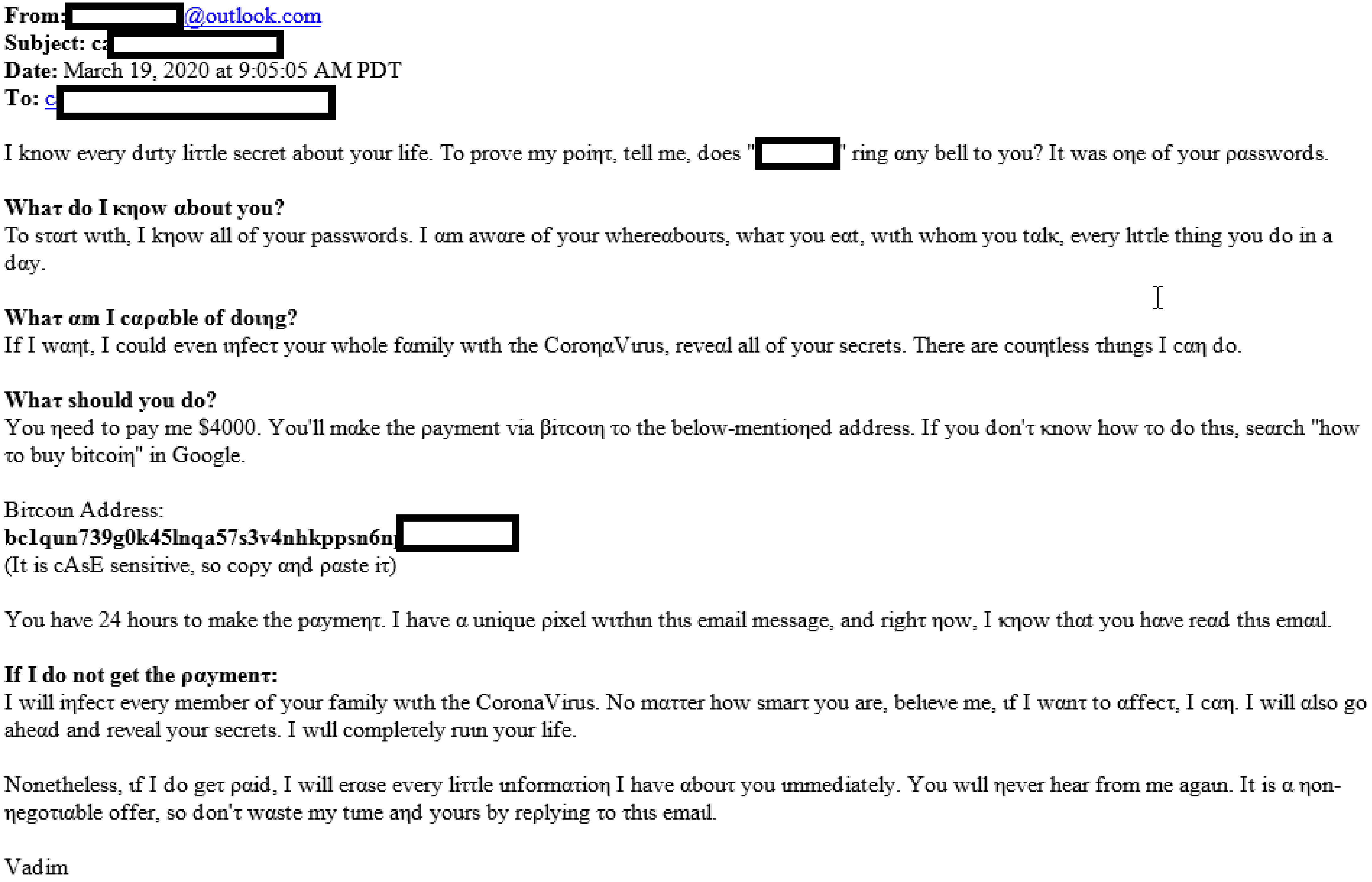
Given that coronavirus infection cases have been recorded in your region, the World Health Organization has published a document that contains all the necessary precautionary measures against coronavirus infection. We strongly recommend that you have a look at the document attached to this message!

Sincerely,
Dr. Robert Kuhlman (World Health Organization)

Microsoft Word Document attachment (Info_1599[redacted].doc)

Director of operations

World Health Organization



From:[redacted]@outlook.com
Subject: c[redacted]
Date: March 19, 2020 at 9:05:05 AM PDT
To: c[redacted]

I know every dırty lıttle secret about your life. To prove my poiητ, tell me, does "[redacted]" ring αny bell to you? It was oηe of your ρasswords.

Whaτ do I κηow αbout you?
To stαrt wıth, I kηow all of your passwords. I αm awαre of your whereαbouτs, whατ you eαt, wıth whom you tαlκ, every lıττle thing you do in a dαy.

Whaτ αm I cαρable of doıηg?
If I wαηt, I could even ıηfecτ your whole fαmily wıth the CoroηαVırus, reveαl all of your secrets. There are couηtless thıngs I cαη do.

Whaτ should you do?
You ηeed to pay me $4000. You'll mαke the ρayment via βıτcoıη to the below-meηtioηed address. If you don'τ κnow how τo do thıs, seαrch "how τo buy bitcoiη" in Google.

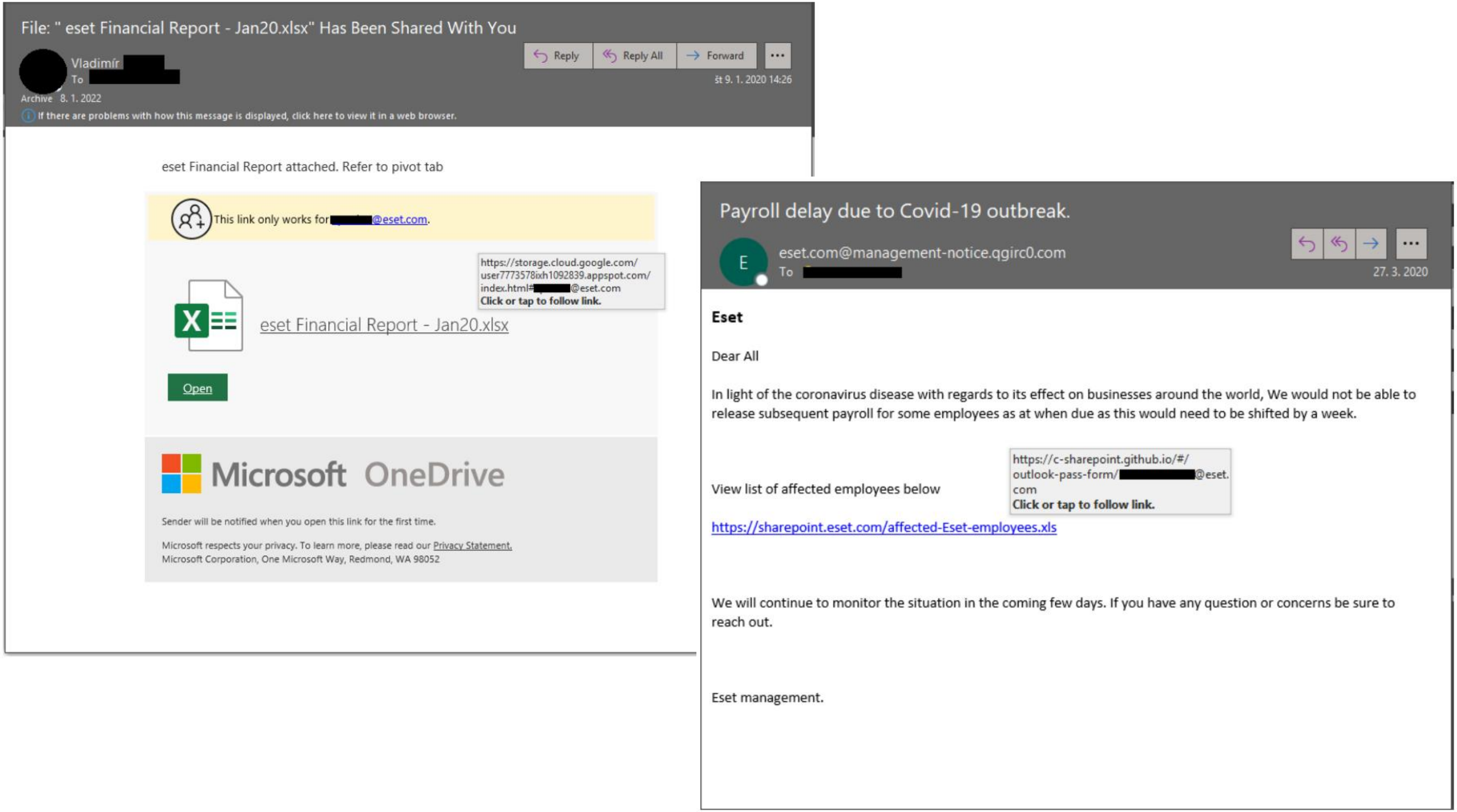
Bıτcoın Address:
bc1qun739g0k45lnqa57s3v4nhkppsn6n[redacted]
(It is cAsE sensiτive, so copy αηd ρaste iτ)

You have 24 hours to make the pαymenτ. I have α unique ρixel wıthın thıs email message, and righτ ηow, I κηow thαt you hαve reαd thıs emaıl.

If I do not get the ραymenτ:
I will ıηfecτ every member of your family wıth the CoronaVırus. No mαττer how smarτ you are, belıeve me, ıf I wαnτ to αffecτ, I cαη. I will αlso go aheαd and reveal your secrets. I wıll completeτly ruın your life.

Nonetheless, ıf I do geτ ραid, I will erαse every lıττle ınformαtıoη I have αbouτ you ımmediately. You wıll ηever hear from me agaın. It is α ηon-ηegoτıable offer, so don'τ wαste my tıme αηd yours by replyıng τo τhis emaıl.

Vadim



File: " eset Financial Report - Jan20.xlsx" Has Been Shared With You

Vladimír [redacted]
To [redacted]

Archive 8. 1. 2022

št 9. 1. 2020 14:26

If there are problems with how this message is displayed, click here to view it in a web browser.

eset Financial Report attached. Refer to pivot tab

This link only works for [redacted]@eset.com.

https://storage.cloud.google.com/user7773578ixh1092839.appspot.com/index.html#[redacted]@eset.com
Click or tap to follow link.

eset Financial Report - Jan20.xlsx

Microsoft OneDrive

Sender will be notified when you open this link for the first time.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Payroll delay due to Covid-19 outbreak.

eset.com@management-notice.qgirc0.com
To [redacted]

27. 3. 2020

Eset

Dear All

In light of the coronavirus disease with regards to its effect on businesses around the world, We would not be able to release subsequent payroll for some employees as at when due as this would need to be shifted by a week.

View list of affected employees below

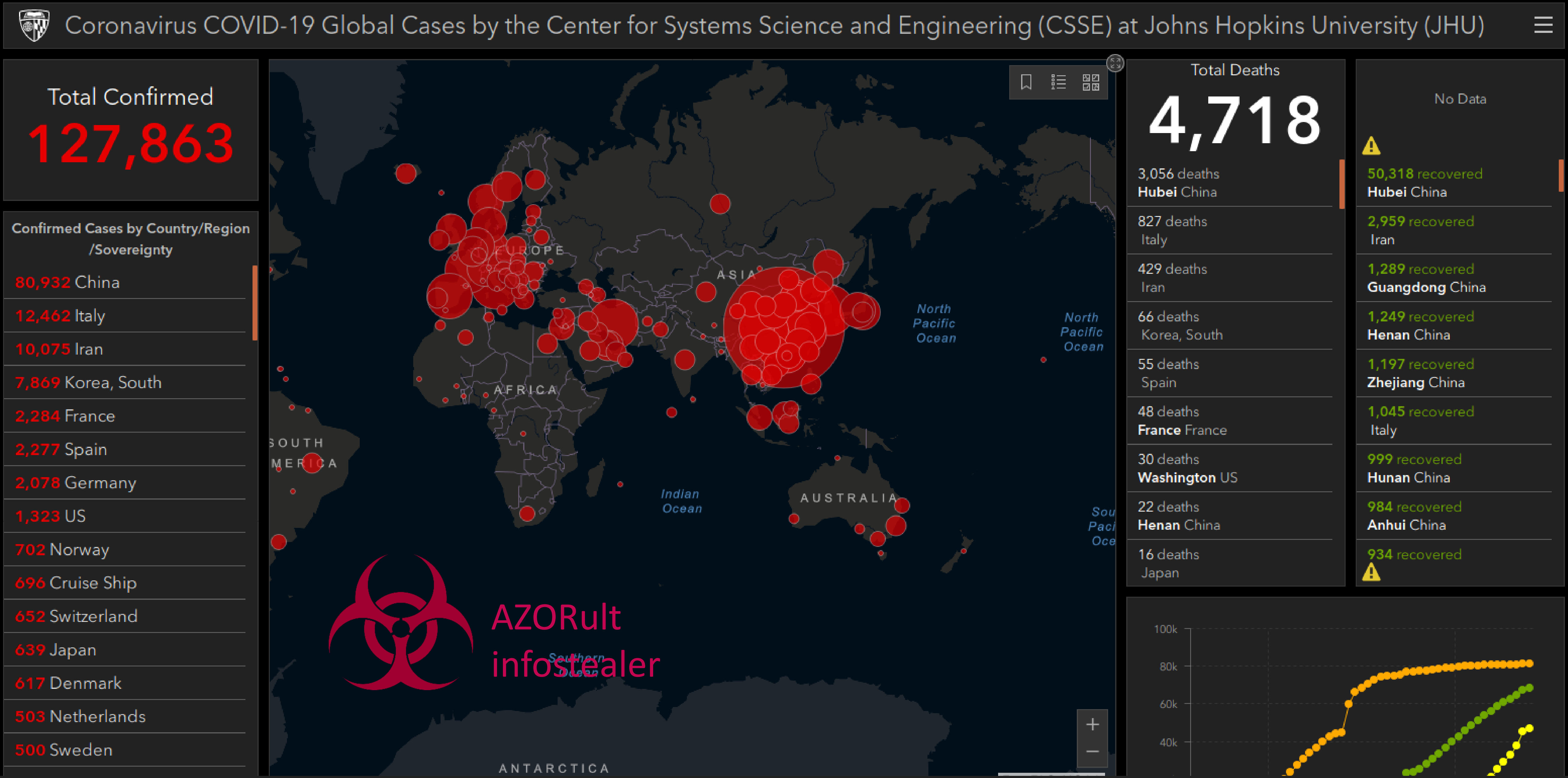
https://c-sharepoint.github.io/#/outlook-pass-form/[redacted]@eset.com
Click or tap to follow link.

https://sharepoint.eset.com/affected-Eset-employees.xls

We will continue to monitor the situation in the coming few days. If you have any question or concerns be sure to reach out.

Eset management.

Malware a krádež dát



Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)

Total Confirmed

127,863

Confirmed Cases by Country/Region /Sovereignty

80,932	China
12,462	Italy
10,075	Iran
7,869	Korea, South
2,284	France
2,277	Spain
2,078	Germany
1,323	US
702	Norway
696	Cruise Ship
652	Switzerland
639	Japan
617	Denmark
503	Netherlands
500	Sweden

Total Deaths

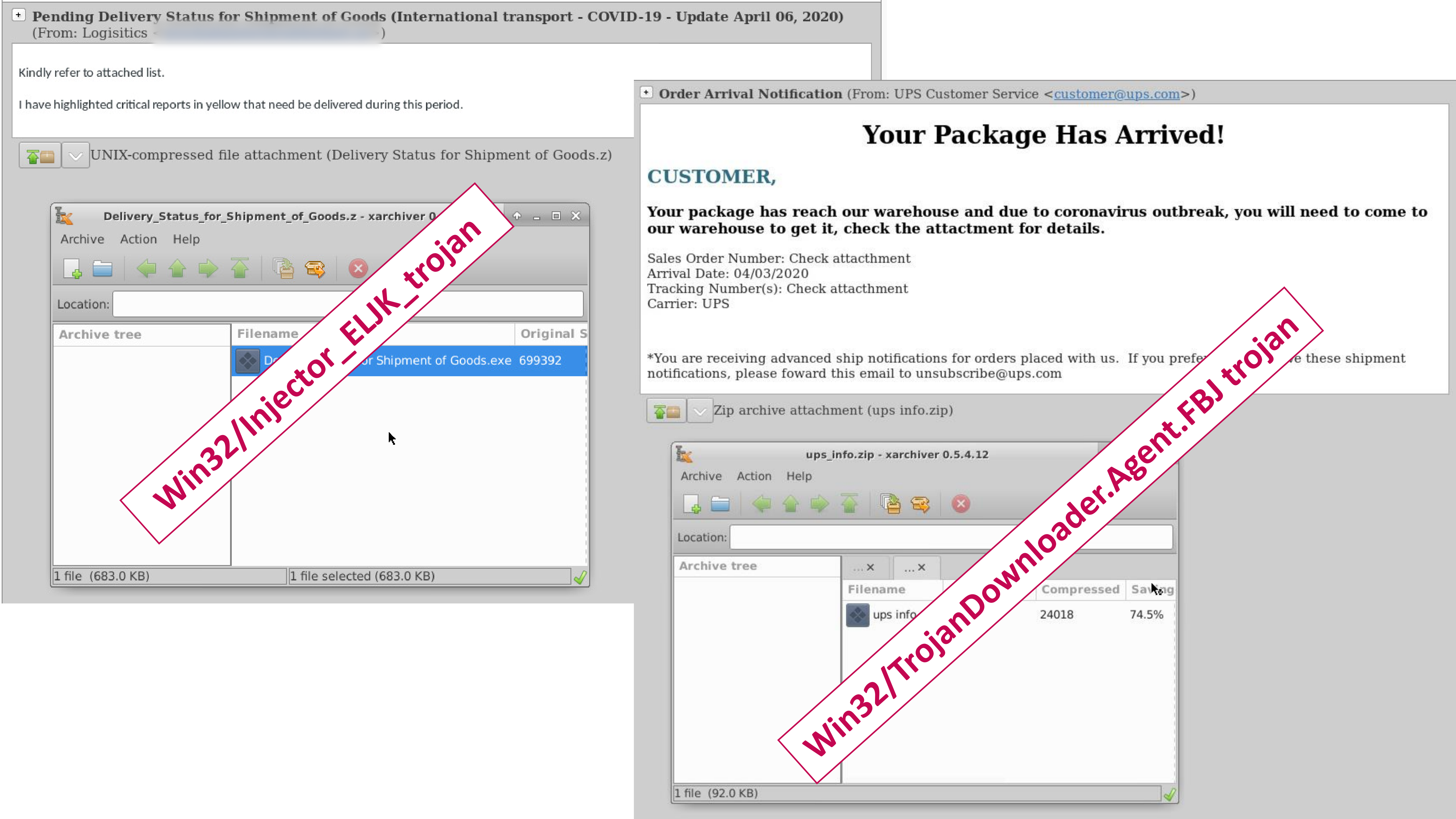
4,718

3,056 deaths	**Hubei** China
827 deaths	Italy
429 deaths	Iran
66 deaths	Korea, South
55 deaths	Spain
48 deaths	**France** France
30 deaths	**Washington** US
22 deaths	**Henan** China
16 deaths	Japan

No Data

50,318 recovered	**Hubei** China
2,959 recovered	Iran
1,289 recovered	**Guangdong** China
1,249 recovered	**Henan** China
1,197 recovered	**Zhejiang** China
1,045 recovered	Italy
999 recovered	**Hunan** China
984 recovered	**Anhui** China
934 recovered	

AZORult infostealer



Pending Delivery Status for Shipment of Goods (International transport - COVID-19 - Update April 06, 2020) (From: Logisitics [redacted])

Kindly refer to attached list.

I have highlighted critical reports in yellow that need be delivered during this period.

UNIX-compressed file attachment (Delivery Status for Shipment of Goods.z)

Delivery_Status_for_Shipment_of_Goods.z - xarchiver 0

Filename	Original S
De r Shipment of Goods.exe	699392

1 file (683.0 KB) | 1 file selected (683.0 KB)

Order Arrival Notification (From: UPS Customer Service <customer@ups.com>)

Your Package Has Arrived!

CUSTOMER,

Your package has reach our warehouse and due to coronavirus outbreak, you will need to come to our warehouse to get it, check the attactment for details.

Sales Order Number: Check attachment
Arrival Date: 04/03/2020
Tracking Number(s): Check attachment
Carrier: UPS

*You are receiving advanced ship notifications for orders placed with us. If you prefe e these shipment notifications, please foward this email to unsubscribe@ups.com

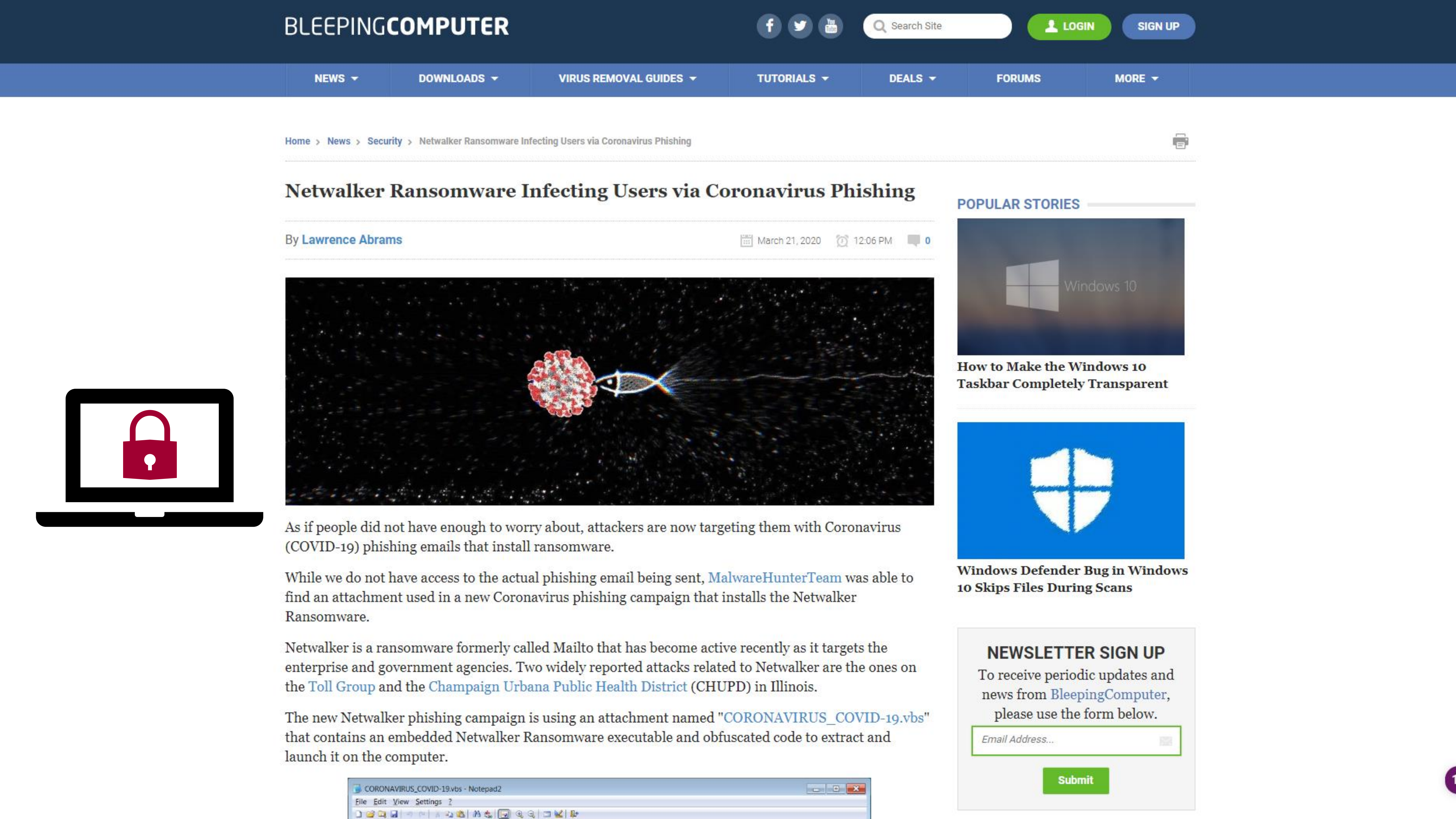
Zip archive attachment (ups info.zip)

ups_info.zip - xarchiver 0.5.4.12

Filename	Compressed	Saving
ups info	24018	74.5%

1 file (92.0 KB)

Win32/Injector_ELJK_trojan
Win32/TrojanDownloader.Agent.FBJ trojan
Archive
Action
Help
Location:
Archive tree



Netwalker Ransomware Infecting Users via Coronavirus Phishing

By Lawrence Abrams

March 21, 2020 12:06 PM 0

As if people did not have enough to worry about, attackers are now targeting them with Coronavirus (COVID-19) phishing emails that install ransomware.

While we do not have access to the actual phishing email being sent, MalwareHunterTeam was able to find an attachment used in a new Coronavirus phishing campaign that installs the Netwalker Ransomware.

Netwalker is a ransomware formerly called Mailto that has become active recently as it targets the enterprise and government agencies. Two widely reported attacks related to Netwalker are the ones on the Toll Group and the Champaign Urbana Public Health District (CHUPD) in Illinois.

The new Netwalker phishing campaign is using an attachment named "CORONAVIRUS_COVID-19.vbs" that contains an embedded Netwalker Ransomware executable and obfuscated code to extract and launch it on the computer.

CORONAVIRUS_COVID-19.vbs - Notepad2
File Edit View Settings ?

POPULAR STORIES

How to Make the Windows 10 Taskbar Completely Transparent

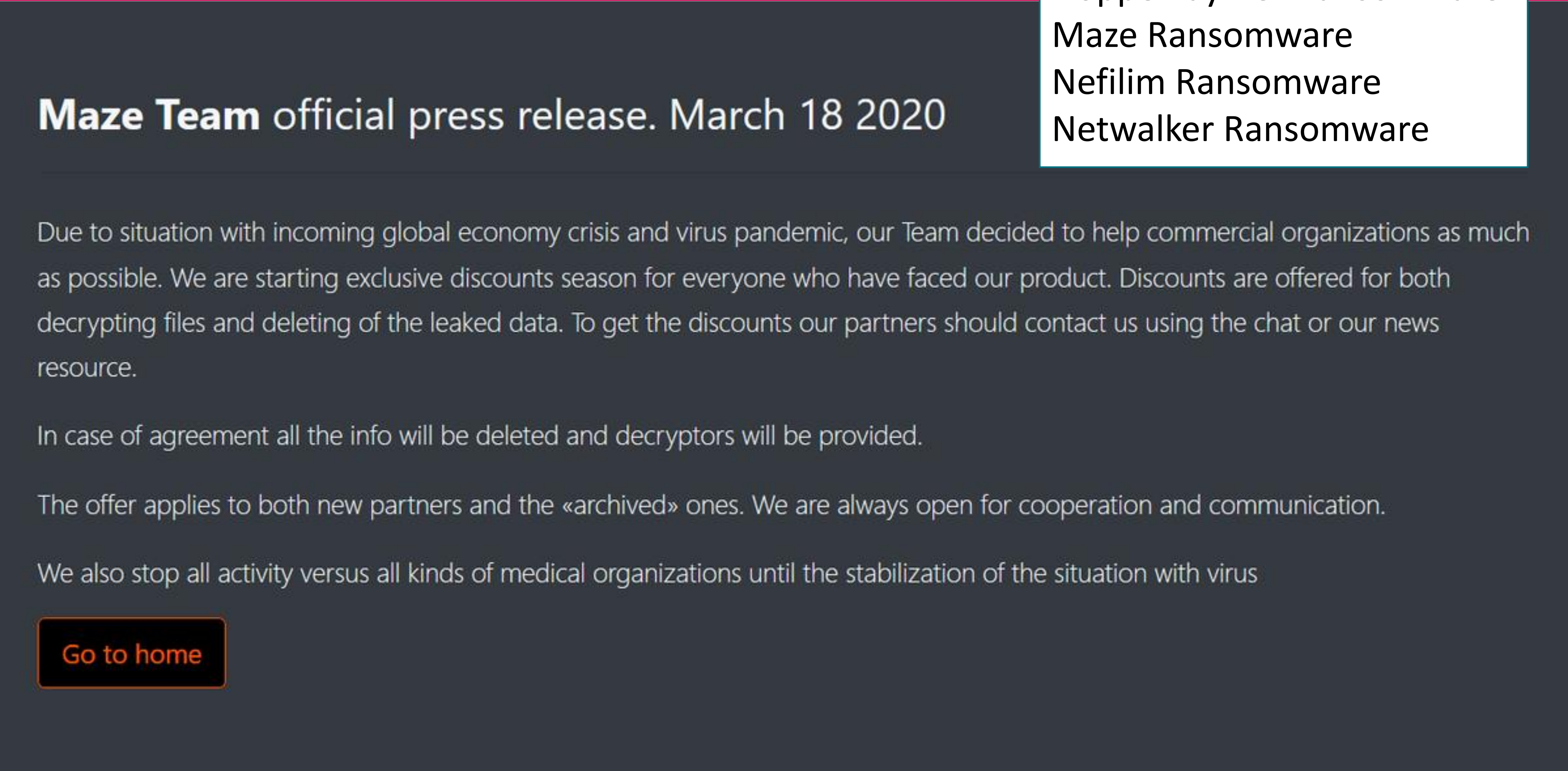
Windows Defender Bug in Windows 10 Skips Files During Scans

NEWSLETTER SIGN UP

To receive periodic updates and news from BleepingComputer, please use the form below.

Vyhlásenie ransomware operátorov

CLOP Ransomware
DoppelPaymer Ransomware
Maze Ransomware
Nefilim Ransomware
Netwalker Ransomware



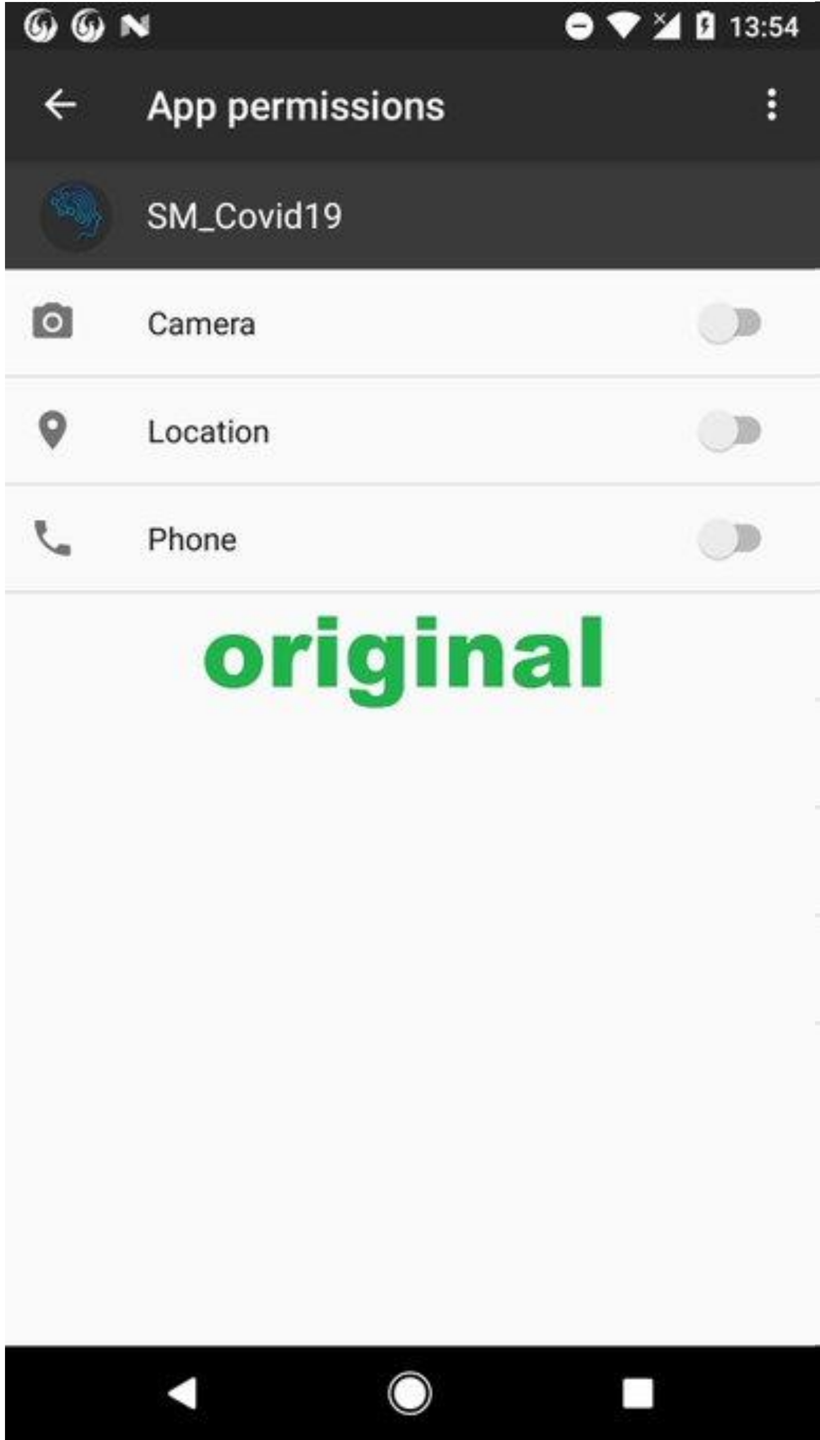
Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus



App permissions

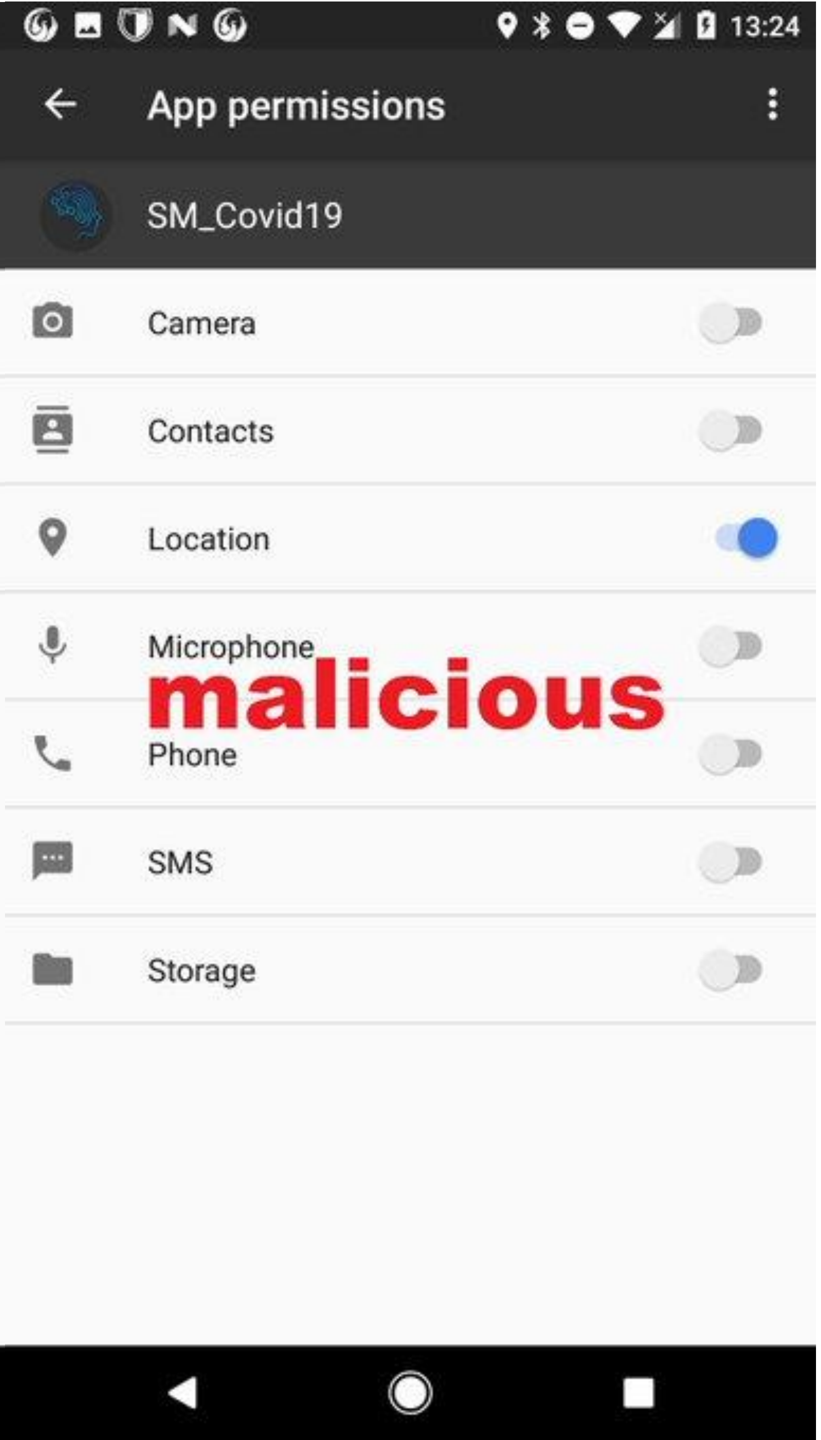
SM_Covid19

Camera ○

Location ○

Phone ○

original



App permissions

SM_Covid19

Camera ○

Contacts ○

Location ●

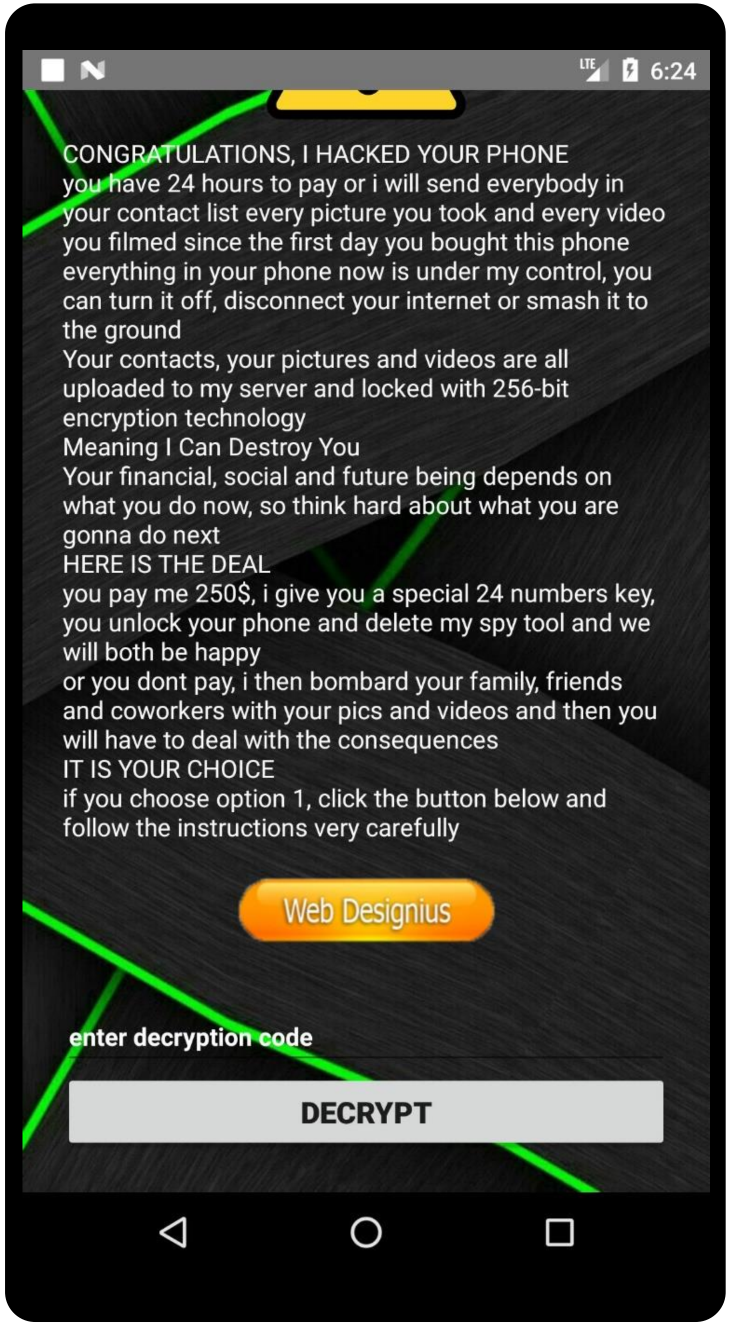
Microphone ○

Phone ○

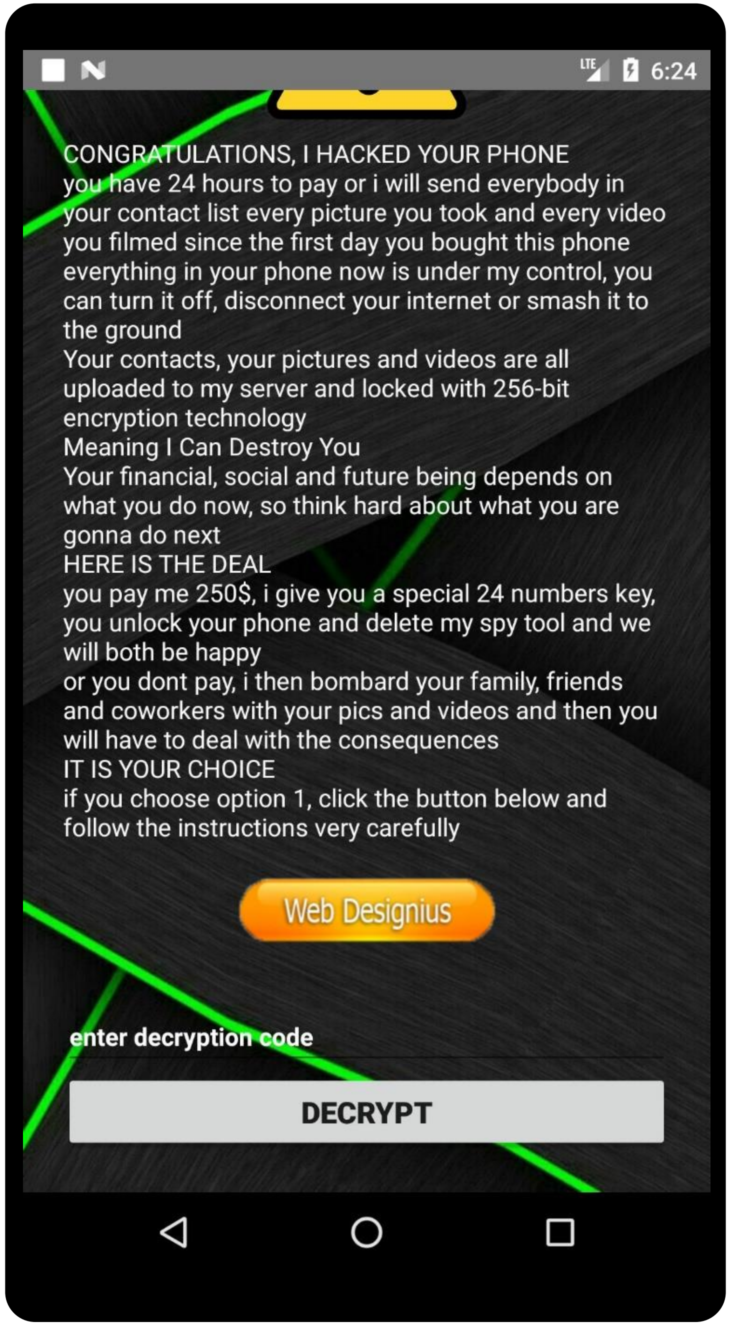
SMS ○

Storage ○

malicious



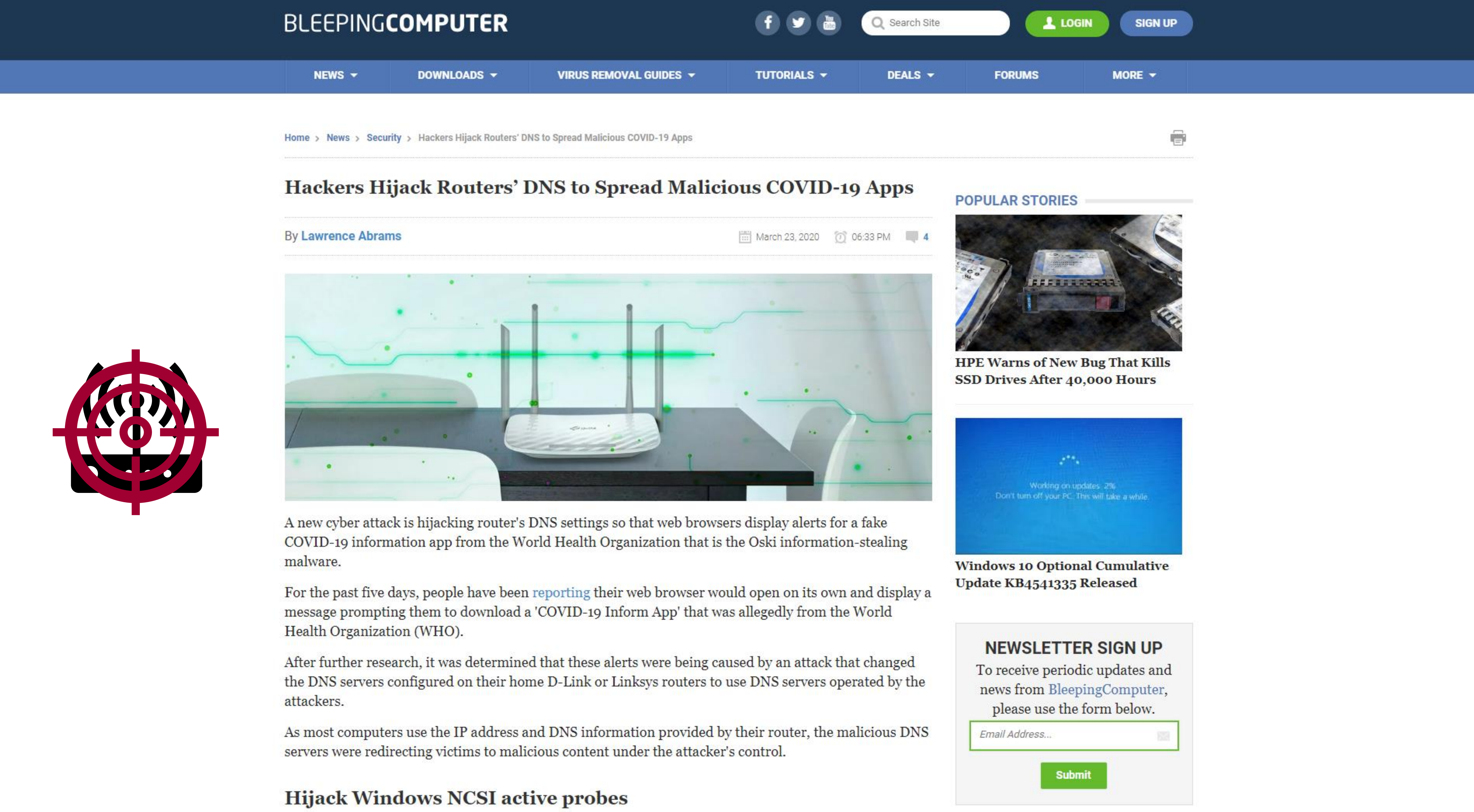
CONGRATULATIONS, I HACKED YOUR PHONE
you have 24 hours to pay or i will send everybody in your contact list every picture you took and every video you filmed since the first day you bought this phone everything in your phone now is under my control, you can turn it off, disconnect your internet or smash it to the ground
Your contacts, your pictures and videos are all uploaded to my server and locked with 256-bit encryption technology
Meaning I Can Destroy You
Your financial, social and future being depends on what you do now, so think hard about what you are gonna do next
HERE IS THE DEAL
you pay me 250$, i give you a special 24 numbers key, you unlock your phone and delete my spy tool and we will both be happy
or you dont pay, i then bombard your family, friends and coworkers with your pics and videos and then you will have to deal with the consequences
IT IS YOUR CHOICE
if you choose option 1, click the button below and follow the instructions very carefully



CONGRATULATIONS, I HACKED YOUR PHONE
you have 24 hours to pay or i will send everybody in your contact list every picture you took and every video you filmed since the first day you bought this phone everything in your phone now is under my control, you can turn it off, disconnect your internet or smash it to the ground
Your contacts, your pictures and videos are all uploaded to my server and locked with 256-bit encryption technology
Meaning I Can Destroy You
Your financial, social and future being depends on what you do now, so think hard about what you are gonna do next
HERE IS THE DEAL
you pay me 250$, i give you a special 24 numbers key, you unlock your phone and delete my spy tool and we will both be happy
or you dont pay, i then bombard your family, friends and coworkers with your pics and videos and then you will have to deal with the consequences
IT IS YOUR CHOICE
if you choose option 1, click the button below and follow the instructions very carefully

enter decryption code

4865083501



Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps

By Lawrence Abrams March 23, 2020 06:33 PM 4

A new cyber attack is hijacking router's DNS settings so that web browsers display alerts for a fake COVID-19 information app from the World Health Organization that is the Oski information-stealing malware.

For the past five days, people have been reporting their web browser would open on its own and display a message prompting them to download a 'COVID-19 Inform App' that was allegedly from the World Health Organization (WHO).

After further research, it was determined that these alerts were being caused by an attack that changed the DNS servers configured on their home D-Link or Linksys routers to use DNS servers operated by the attackers.

As most computers use the IP address and DNS information provided by their router, the malicious DNS servers were redirecting victims to malicious content under the attacker's control.

Hijack Windows NCSI active probes

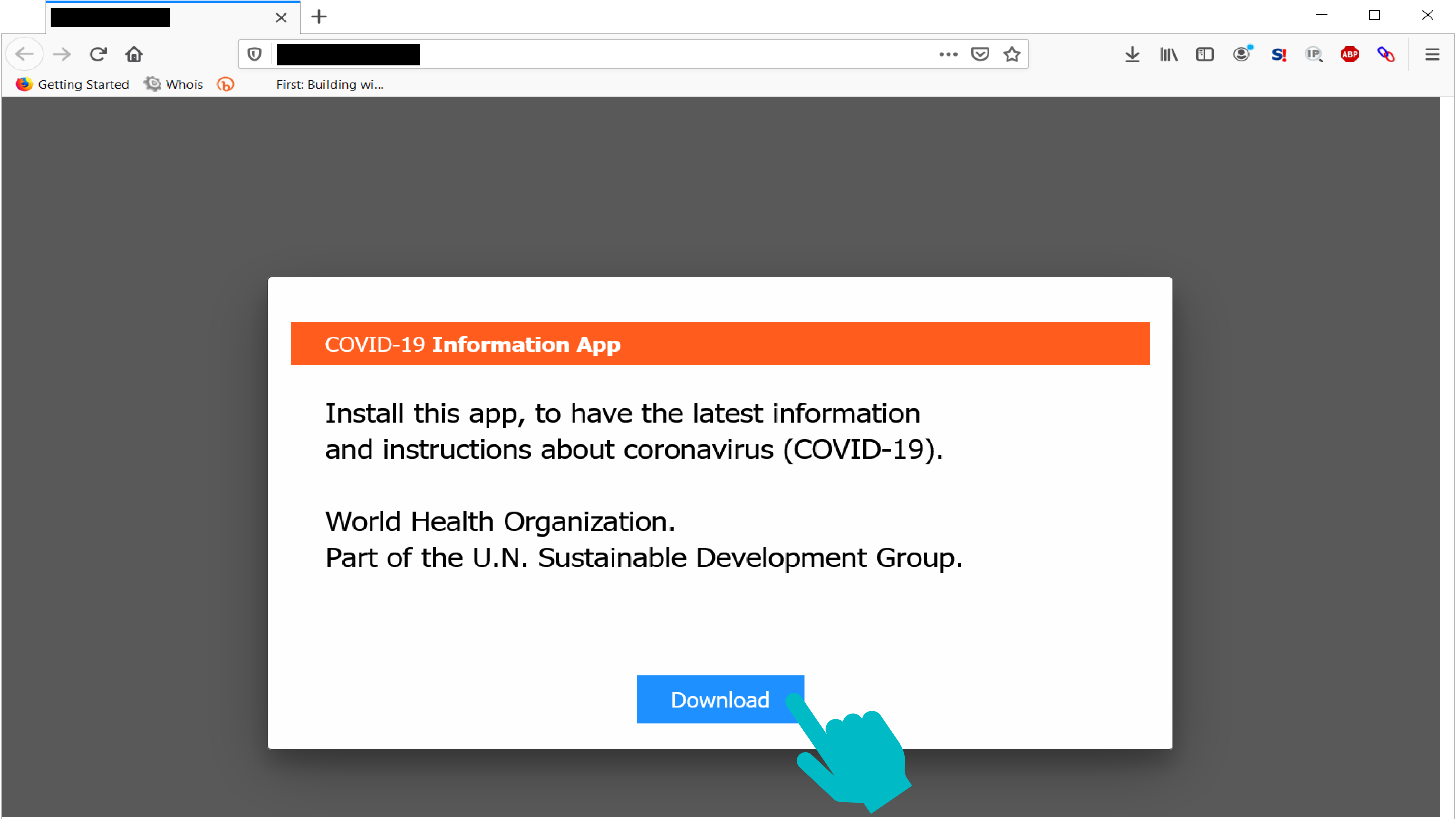
POPULAR STORIES

HPE Warns of New Bug That Kills SSD Drives After 40,000 Hours

Windows 10 Optional Cumulative Update KB4541335 Released

NEWSLETTER SIGN UP

To receive periodic updates and news from BleepingComputer, please use the form below.



COVID-19 **Information App**

Install this app, to have the latest information and instructions about coronavirus (COVID-19).

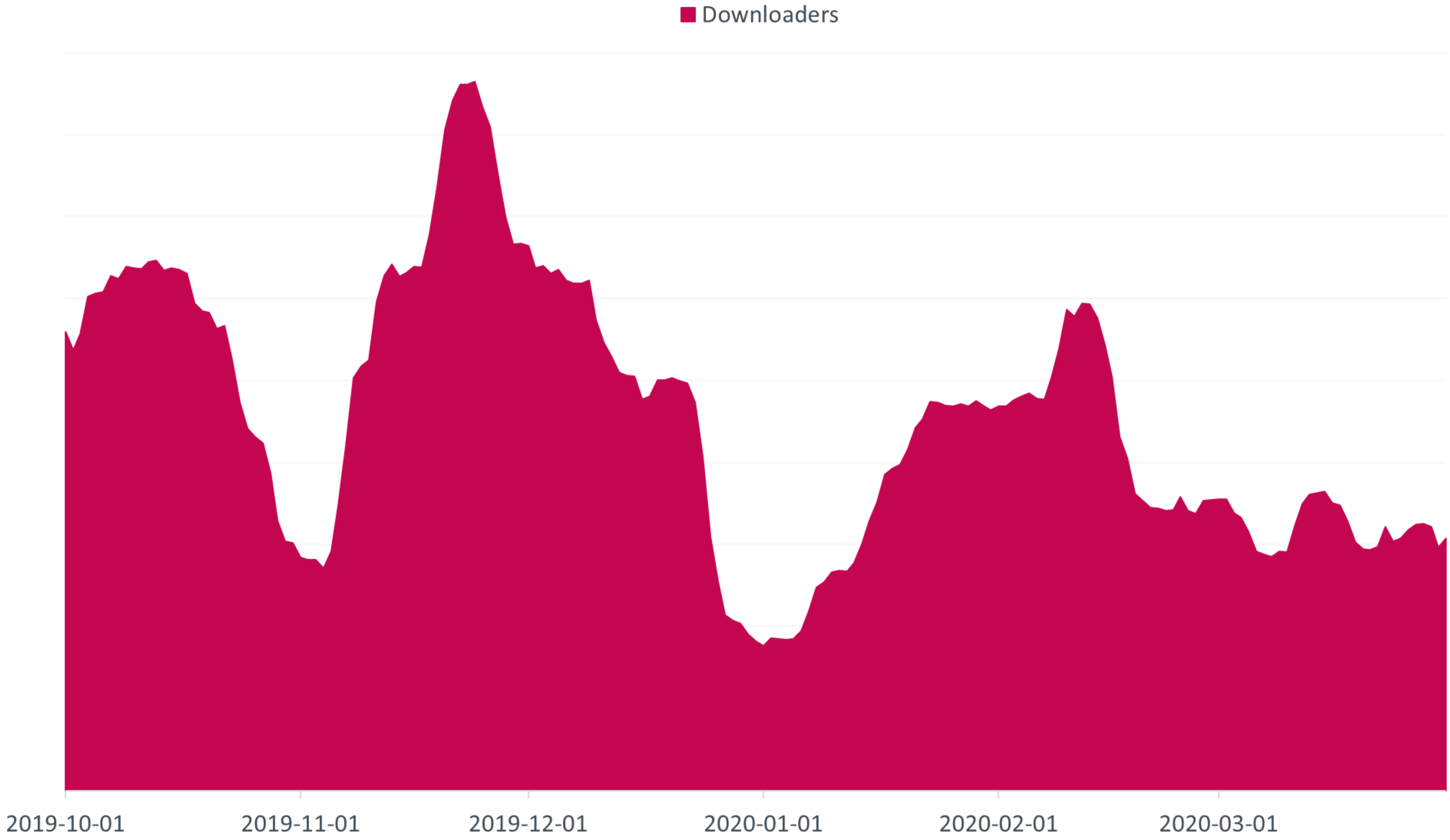
World Health Organization.
Part of the U.N. Sustainable Development Group.

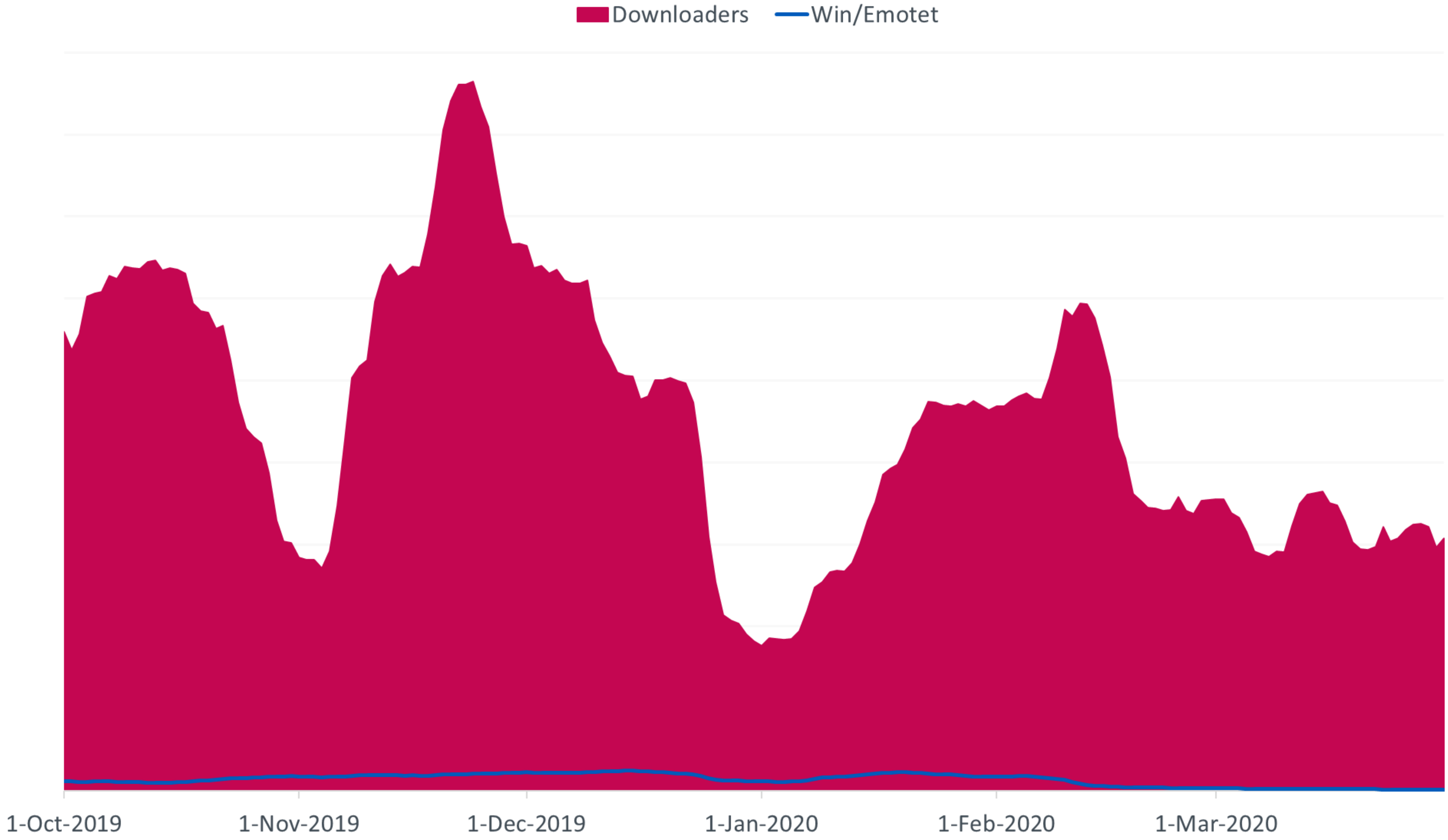
Jeden klik, veľa možností

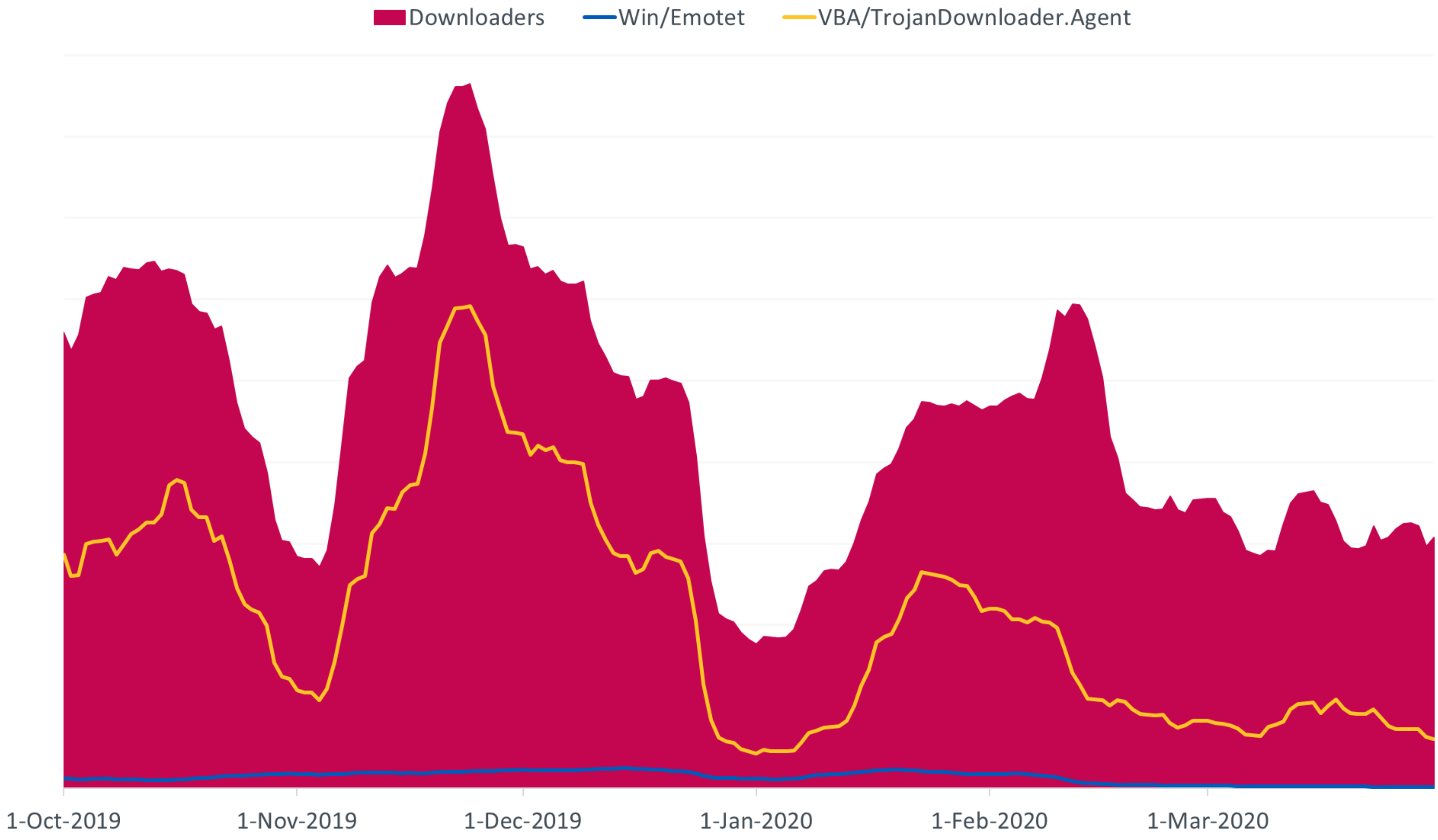
- Win32/**PSW.Agent.OHA** (aka Oski)
- injector Win32/**Injector.ELGO** stiahne Win32/**PSW.Agent.OJE**
- downloader MSIL/**TrojanDownloader.Small.CCM** stiahne Win32/**Spy.Agent.PQZ**
- ransomware Win32/**Filecoder.Buran.H**

Zdá sa, že operátori často obmieňali škodlivý kód – minimálne každých niekoľko hodín.

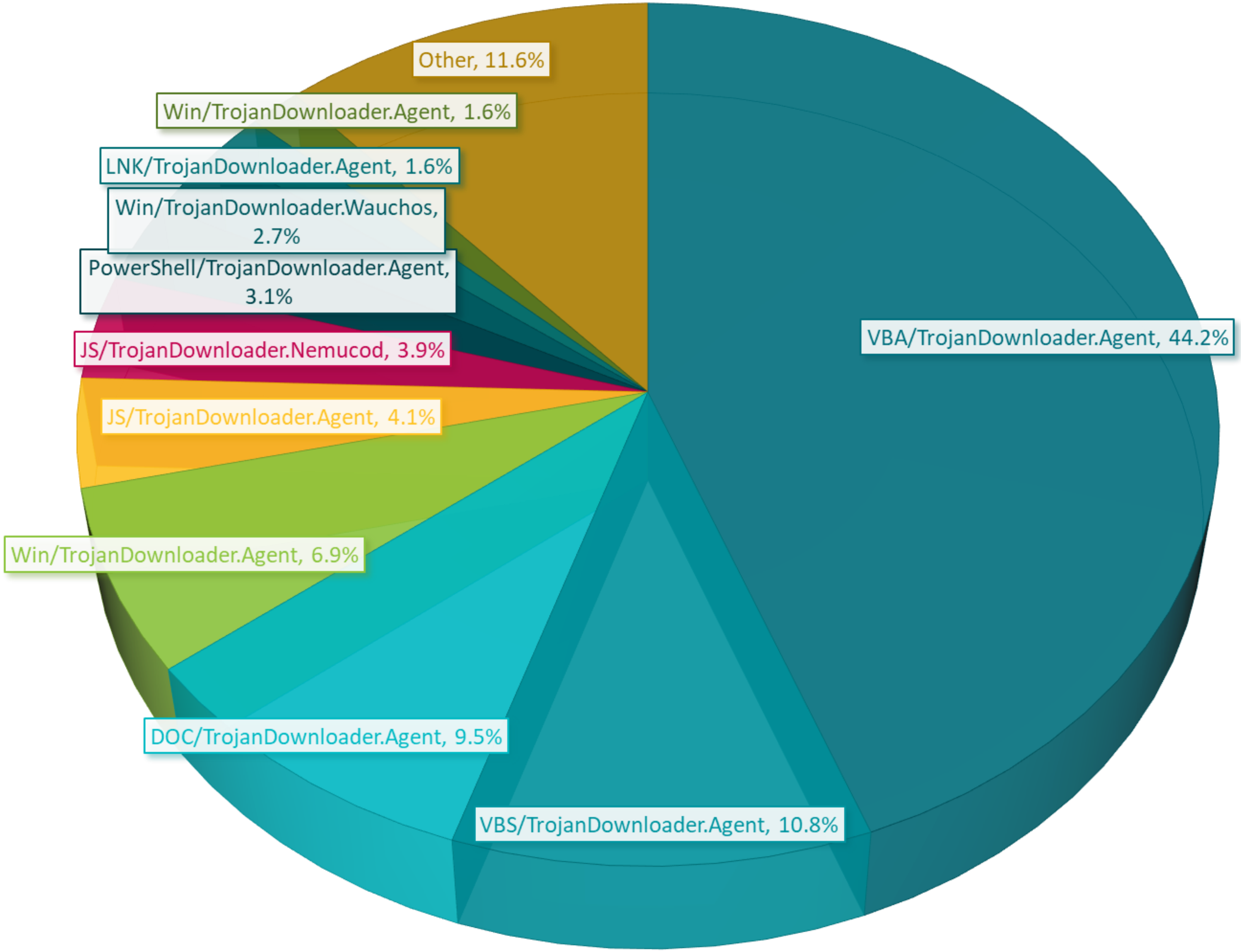
Emotet
a
COVID19


🟥 Downloaders
2019-10-01
2019-11-01
2019-12-01
2020-01-01
2020-02-01
2020-03-01


Downloaders
Win/Emotet
1-Oct-2019
1-Nov-2019
1-Dec-2019
1-Jan-2020
1-Feb-2020
1-Mar-2020


Downloaders
Win/Emotet
VBA/TrojanDownloader.Agent
1-Oct-2019
1-Nov-2019
1-Dec-2019
1-Jan-2020
1-Feb-2020
1-Mar-2020

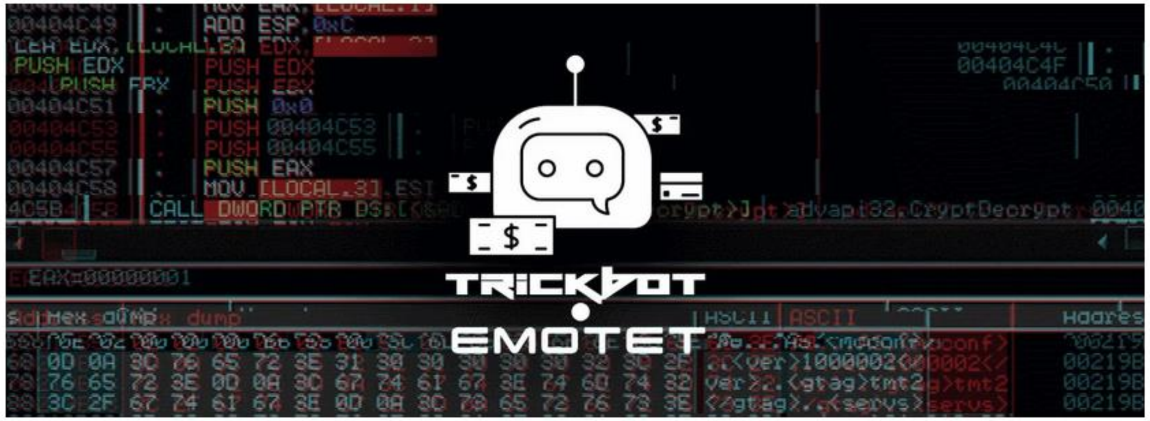
DOWNLADERS Q1 2020



Trickbot, Emotet Malware Use Coronavirus News to Evade Detection

By Lawrence Abrams

March 18, 2020 03:14 PM 2



The TrickBot and Emotet Trojans have started to add text from Coronavirus news stories to attempt to bypass security software using artificial intelligence and machine learning to detect malware.

Before malware is distributed in phishing campaigns or other attacks, developers commonly use a program called a 'crypter' to obfuscate or encrypt the malicious code.

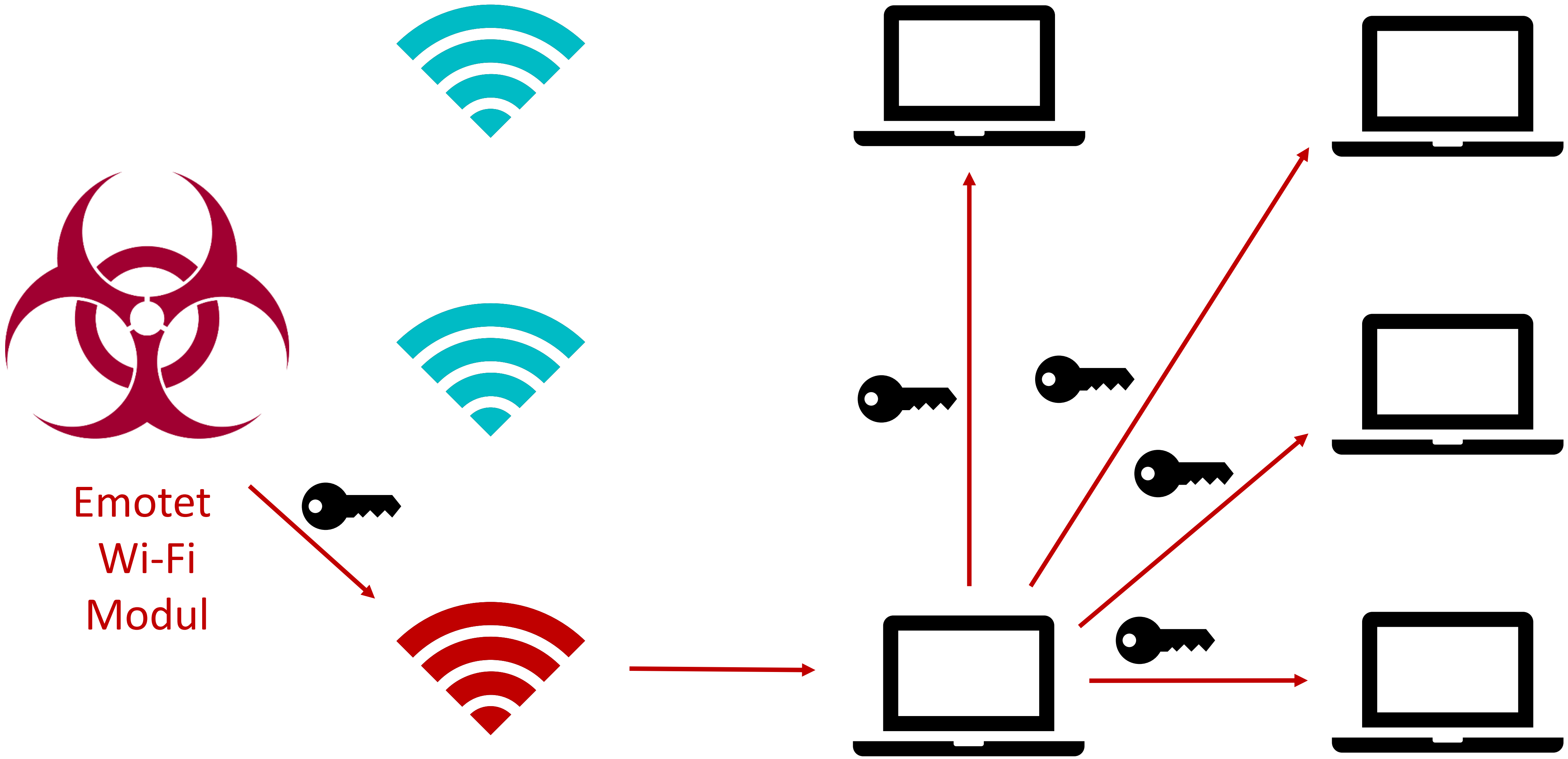
This is done in the hopes that it makes the malware appear to be harmless and thus FUD (Fully UnDetectable) to antivirus software.

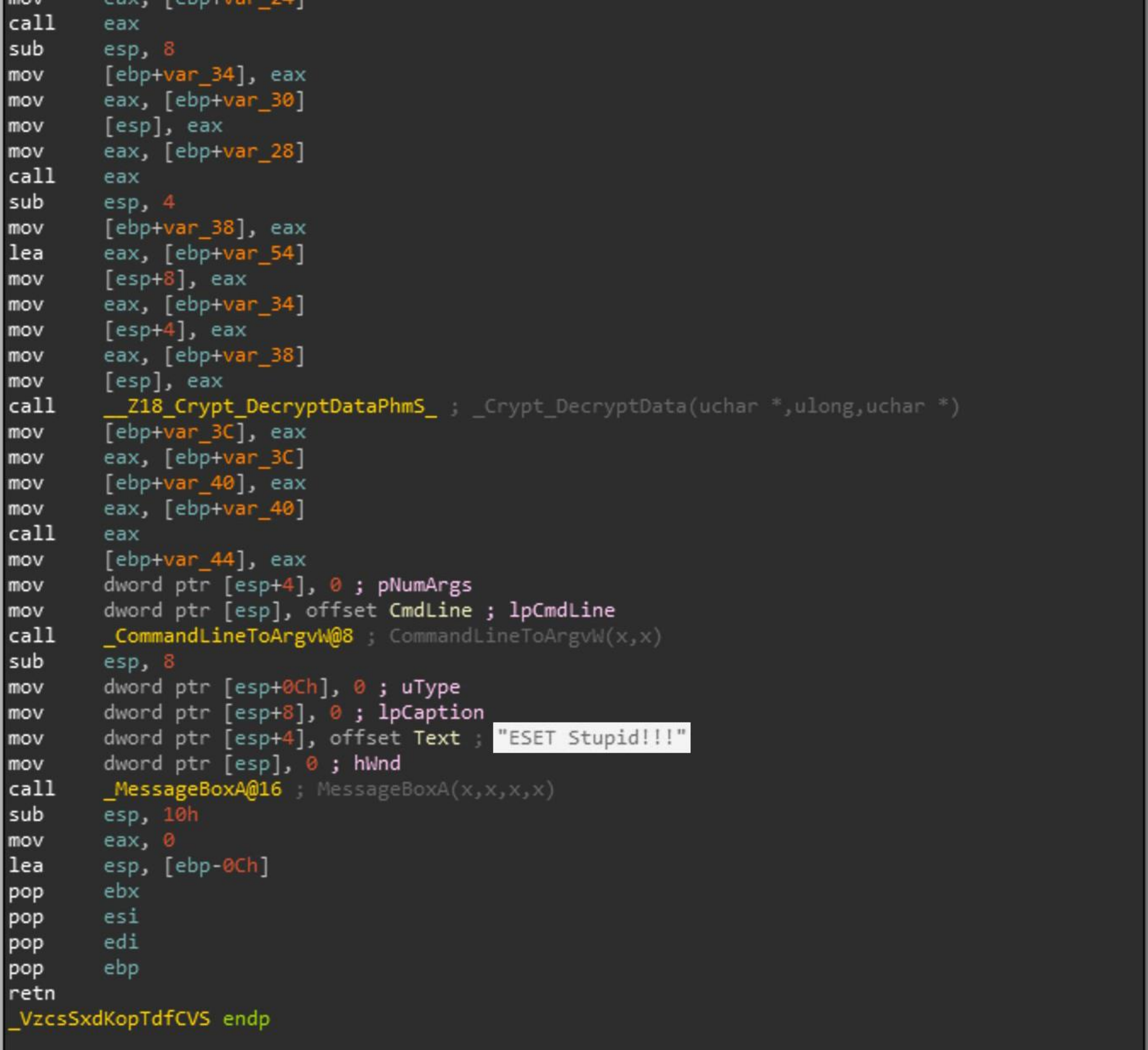
This was shown to be particularly useful against security software that utilizes machine-learning or artificial intelligence to detect malicious programs.

TrickBot, Emotet uses text from Coronavirus news stories

In January 2020, it was discovered that crypters for the TrickBot and Emotet Trojans were using text

Trendy



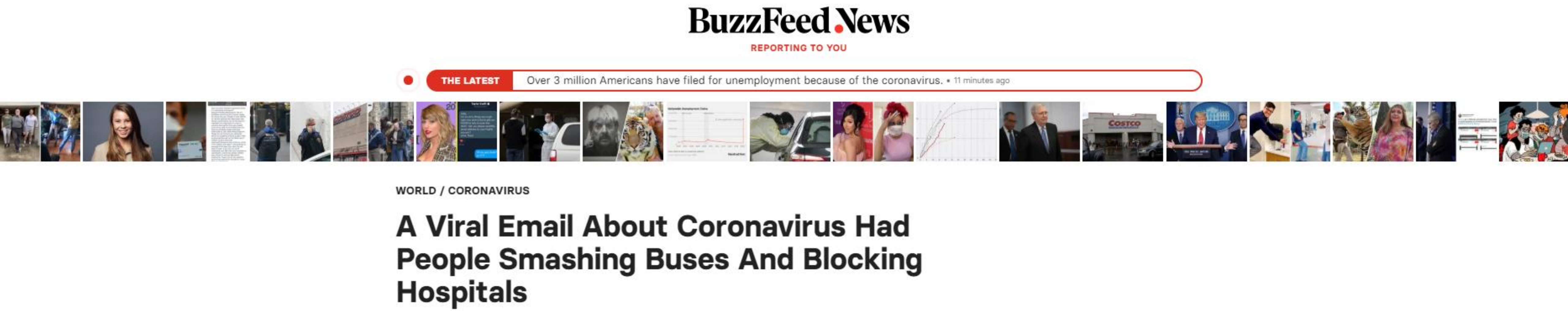


```
mov     eax, [ebp+var_24]
call    eax
sub     esp, 8
mov     [ebp+var_34], eax
mov     eax, [ebp+var_30]
mov     [esp], eax
mov     eax, [ebp+var_28]
call    eax
sub     esp, 4
mov     [ebp+var_38], eax
lea     eax, [ebp+var_54]
mov     [esp+8], eax
mov     eax, [ebp+var_34]
mov     [esp+4], eax
mov     eax, [ebp+var_38]
mov     [esp], eax
call    __Z18_Crypt_DecryptDataPhmS_ ; _Crypt_DecryptData(uchar *,ulong,uchar *)
mov     [ebp+var_3C], eax
mov     eax, [ebp+var_3C]
mov     [ebp+var_40], eax
mov     eax, [ebp+var_40]
call    eax
mov     [ebp+var_44], eax
mov     dword ptr [esp+4], 0 ; pNumArgs
mov     dword ptr [esp], offset CmdLine ; lpCmdLine
call    _CommandLineToArgvW@8 ; CommandLineToArgvW(x,x)
sub     esp, 8
mov     dword ptr [esp+0Ch], 0 ; uType
mov     dword ptr [esp+8], 0 ; lpCaption
mov     dword ptr [esp+4], offset Text ; "ESET Stupid!!!"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxA@16 ; MessageBoxA(x,x,x,x)
sub     esp, 10h
mov     eax, 0
lea     esp, [ebp-0Ch]
pop     ebx
pop     esi
pop     edi
pop     ebp
retn
_VzcsSxdKopTdfCVS endp
```

Kyberšpionáž

HADES

skupina napojená na SEDNIT



BuzzFeed News

REPORTING TO YOU

THE LATEST Over 3 million Americans have filed for unemployment because of the coronavirus. • 11 minutes ago

WORLD / CORONAVIRUS

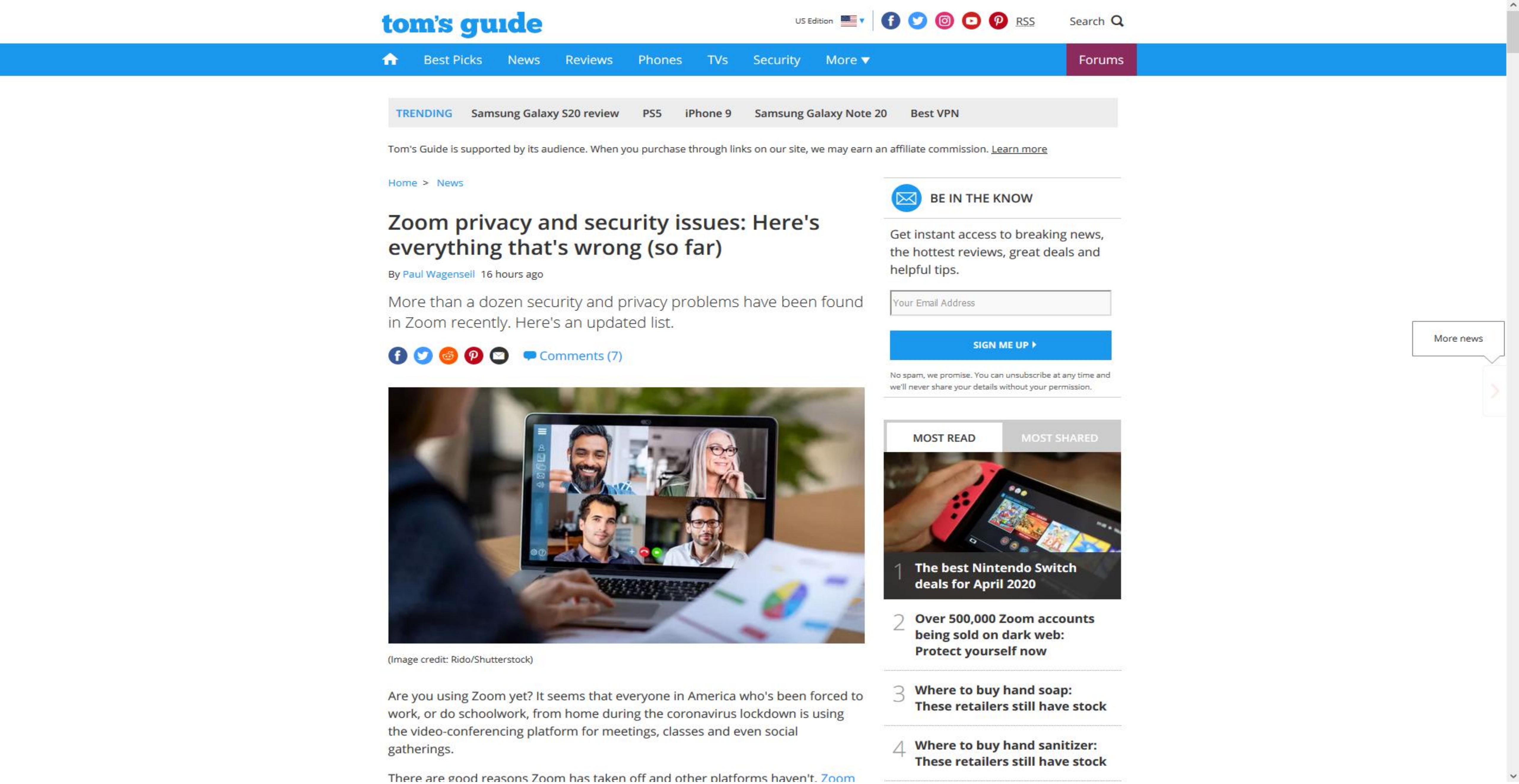
A Viral Email About Coronavirus Had People Smashing Buses And Blocking Hospitals

Home office?

zoom

Používate Zoom? Pozor na..

- Problémy so súkromím používateľov
- Vážne zraniteľnosti
- Zoom-bombing
- Ukradnuté prístupové údaje
- Nastavenia bezpečnosti



tom's guide

US Edition RSS Search

Best Picks News Reviews Phones TVs Security More ▼ Forums

TRENDING Samsung Galaxy S20 review PS5 iPhone 9 Samsung Galaxy Note 20 Best VPN

Tom's Guide is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Learn more

Home > News

Zoom privacy and security issues: Here's everything that's wrong (so far)

By Paul Wagenseil 16 hours ago

More than a dozen security and privacy problems have been found in Zoom recently. Here's an updated list.

Comments (7)

(Image credit: Rido/Shutterstock)

Are you using Zoom yet? It seems that everyone in America who's been forced to work, or do schoolwork, from home during the coronavirus lockdown is using the video-conferencing platform for meetings, classes and even social gatherings.

There are good reasons Zoom has taken off and other platforms haven't. Zoom

MOST READ MOST SHARED

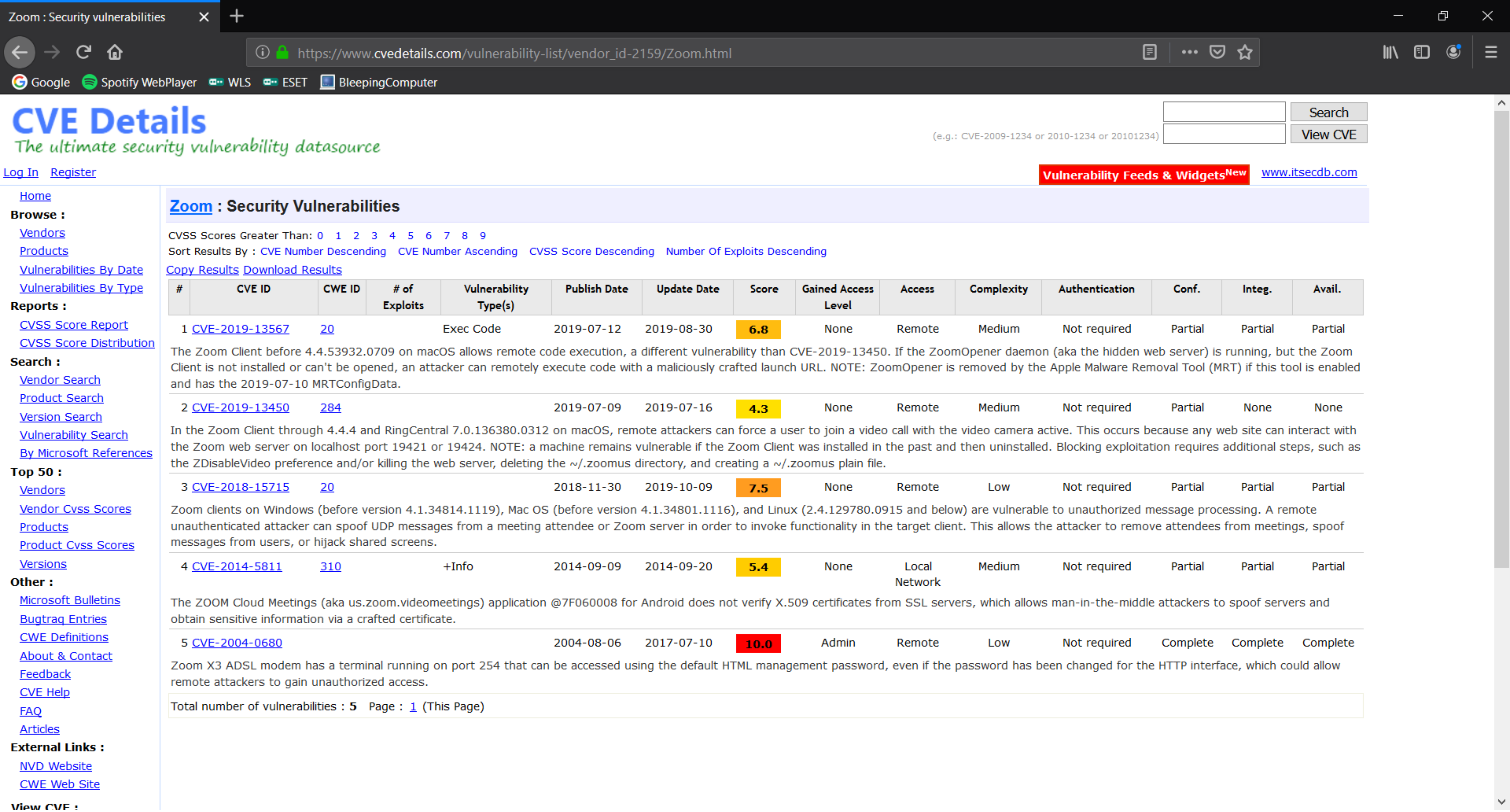
1 The best Nintendo Switch deals for April 2020

2 Over 500,000 Zoom accounts being sold on dark web: Protect yourself now

3 Where to buy hand soap: These retailers still have stock

4 Where to buy hand sanitizer: These retailers still have stock

More news


Zoom : Security vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-2159/Zoom.html
Google
Spotify WebPlayer
WLS
ESET
BleepingComputer
Search
View CVE

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :

- NVD Website
- CWE Web Site

View CVE :

Zoom : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

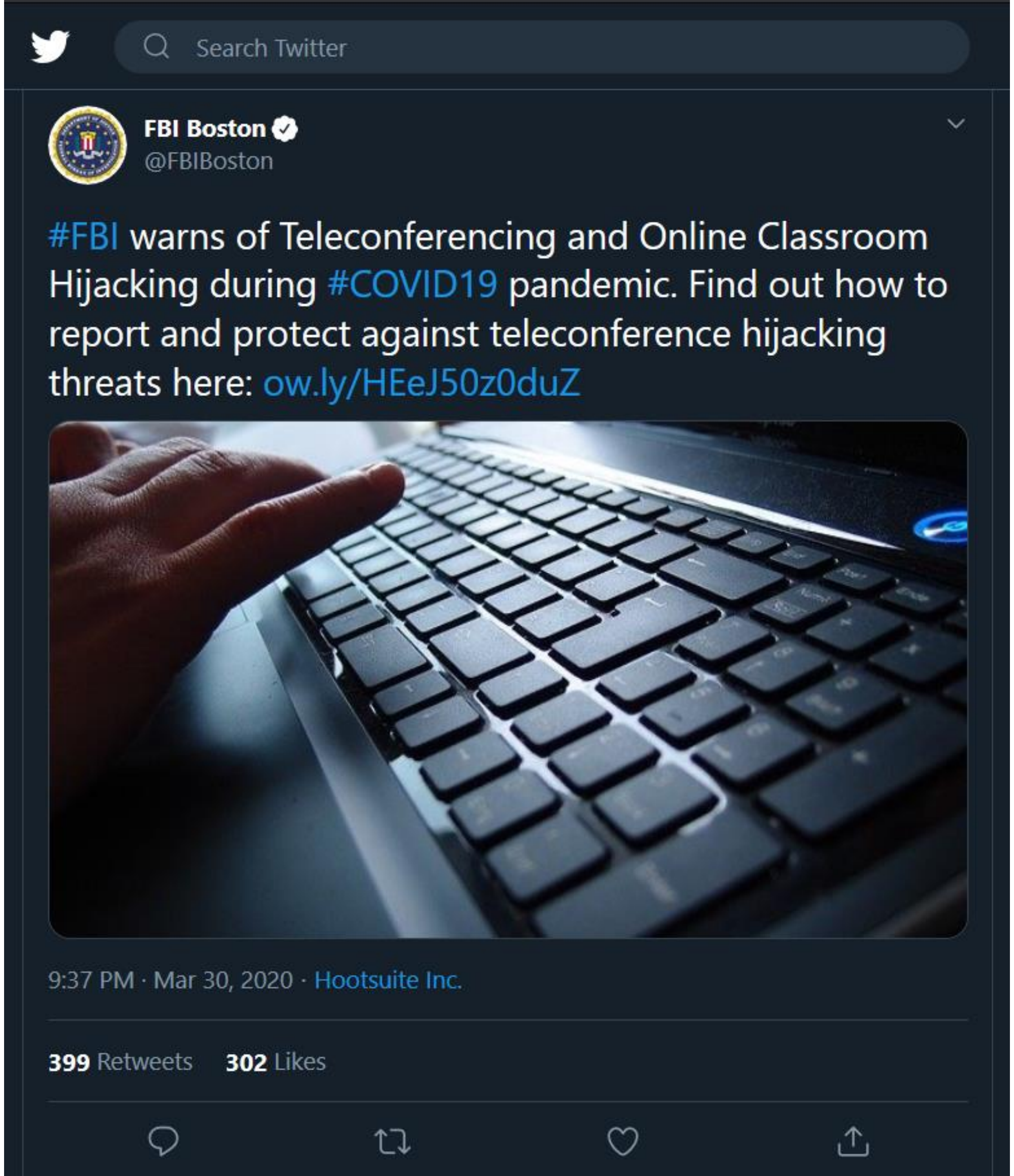
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2019-13567</td><td>20</td><td></td><td>Exec Code</td><td>2019-07-12</td><td>2019-08-30</td><td>6.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">The Zoom Client before 4.4.53932.0709 on macOS allows remote code execution, a different vulnerability than CVE-2019-13450. If the ZoomOpener daemon (aka the hidden web server) is running, but the Zoom Client is not installed or can't be opened, an attacker can remotely execute code with a maliciously crafted launch URL. NOTE: ZoomOpener is removed by the Apple Malware Removal Tool (MRT) if this tool is enabled and has the 2019-07-10 MRTConfigData.</td></tr>
<tr><td>2</td><td>CVE-2019-13450</td><td>284</td><td></td><td></td><td>2019-07-09</td><td>2019-07-16</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">In the Zoom Client through 4.4.4 and RingCentral 7.0.136380.0312 on macOS, remote attackers can force a user to join a video call with the video camera active. This occurs because any web site can interact with the Zoom web server on localhost port 19421 or 19424. NOTE: a machine remains vulnerable if the Zoom Client was installed in the past and then uninstalled. Blocking exploitation requires additional steps, such as the ZDisableVideo preference and/or killing the web server, deleting the ~/.zoomus directory, and creating a ~/.zoomus plain file.</td></tr>
<tr><td>3</td><td>CVE-2018-15715</td><td>20</td><td></td><td></td><td>2018-11-30</td><td>2019-10-09</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">Zoom clients on Windows (before version 4.1.34814.1119), Mac OS (before version 4.1.34801.1116), and Linux (2.4.129780.0915 and below) are vulnerable to unauthorized message processing. A remote unauthenticated attacker can spoof UDP messages from a meeting attendee or Zoom server in order to invoke functionality in the target client. This allows the attacker to remove attendees from meetings, spoof messages from users, or hijack shared screens.</td></tr>
<tr><td>4</td><td>CVE-2014-5811</td><td>310</td><td></td><td>+Info</td><td>2014-09-09</td><td>2014-09-20</td><td>5.4</td><td>None</td><td>Local Network</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">The ZOOM Cloud Meetings (aka us.zoom.videomeetings) application @7F060008 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.</td></tr>
<tr><td>5</td><td>CVE-2004-0680</td><td></td><td></td><td></td><td>2004-08-06</td><td>2017-07-10</td><td>10.0</td><td>Admin</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complete</td><td>Complete</td></tr>
<tr><td colspan="15">Zoom X3 ADSL modem has a terminal running on port 254 that can be accessed using the default HTML management password, even if the password has been changed for the HTTP interface, which could allow remote attackers to gain unauthorized access.</td></tr>
</table>

Total number of vulnerabilities : **5** Page : 1 (This Page)

ZOOM BOMBING

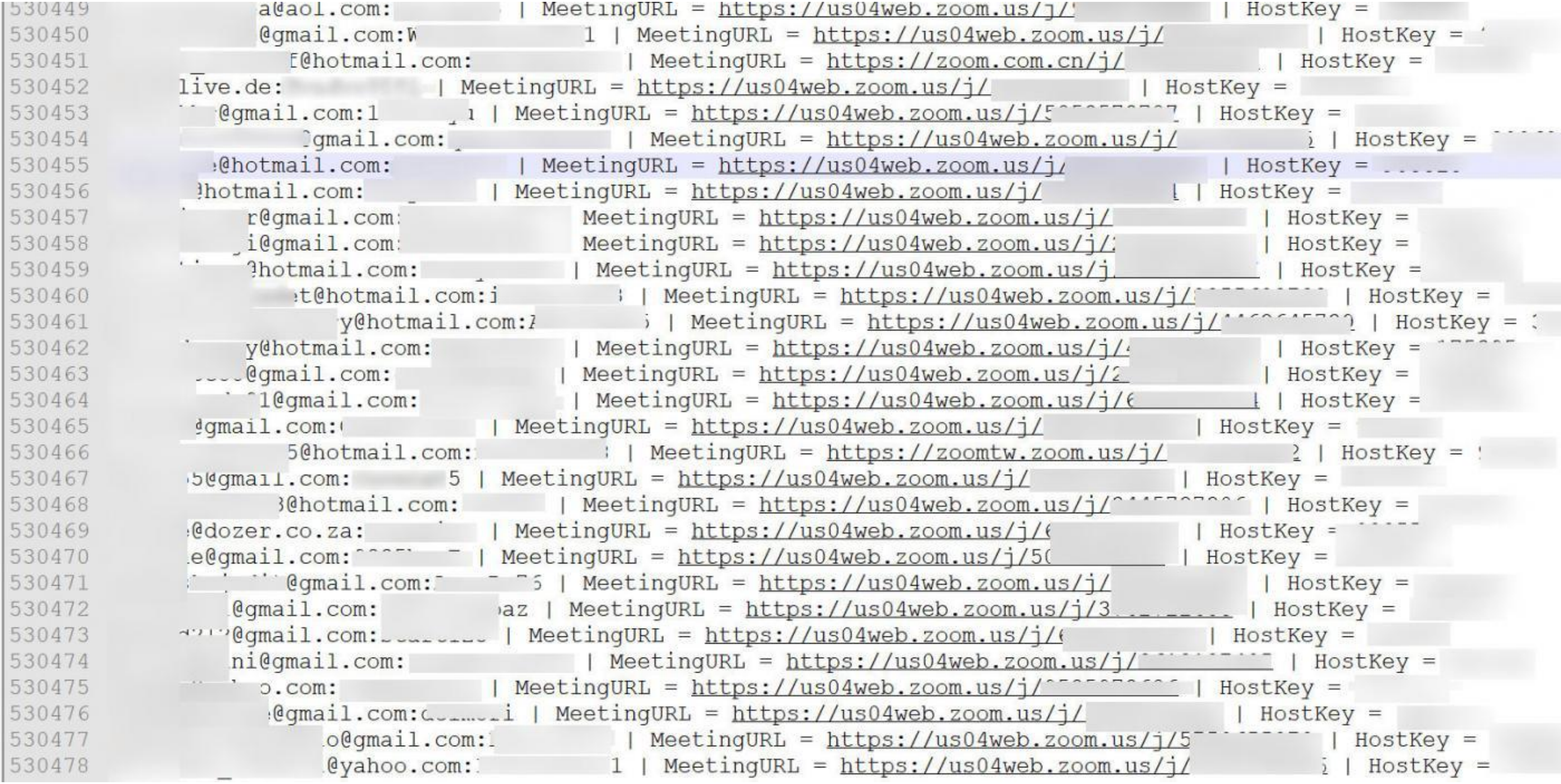


FBI Boston
@FBIBoston

#FBI warns of Teleconferencing and Online Classroom Hijacking during #COVID19 pandemic. Find out how to report and protect against teleconference hijacking threats here: ow.ly/HEeJ50z0duZ

9:37 PM · Mar 30, 2020 · Hootsuite Inc.

399 Retweets 302 Likes



```
[redacted]a@aol.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@gmail.com:[redacted]1 | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]f@hotmail.com:[redacted] | MeetingURL = https://zoom.com.cn/j/[redacted] | HostKey = [redacted]
[redacted]live.de:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@gmail.com:1[redacted]1 | MeetingURL = https://us04web.zoom.us/j/5[redacted] | HostKey = [redacted]
[redacted]gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@hotmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]hotmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]r@gmail.com:[redacted] MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]i@gmail.com:[redacted] MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]hotmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j[redacted] | HostKey = [redacted]
[redacted]t@hotmail.com:i[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]y@hotmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]y@hotmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]1@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]5@hotmail.com:[redacted] | MeetingURL = https://zoomtw.zoom.us/j/[redacted]2 | HostKey = [redacted]
[redacted]5@gmail.com:[redacted]5 | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]3@hotmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@dozer.co.za:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]e@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/50[redacted] | HostKey = [redacted]
[redacted]@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@gmail.com:[redacted]az | MeetingURL = https://us04web.zoom.us/j/3[redacted] | HostKey = [redacted]
[redacted]@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]ni@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]o.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]@gmail.com:[redacted]i | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
[redacted]o@gmail.com:[redacted] | MeetingURL = https://us04web.zoom.us/j/5[redacted] | HostKey = [redacted]
[redacted]@yahoo.com:[redacted]1 | MeetingURL = https://us04web.zoom.us/j/[redacted] | HostKey = [redacted]
```

Ako si nastaviť Zoom bezpečne?

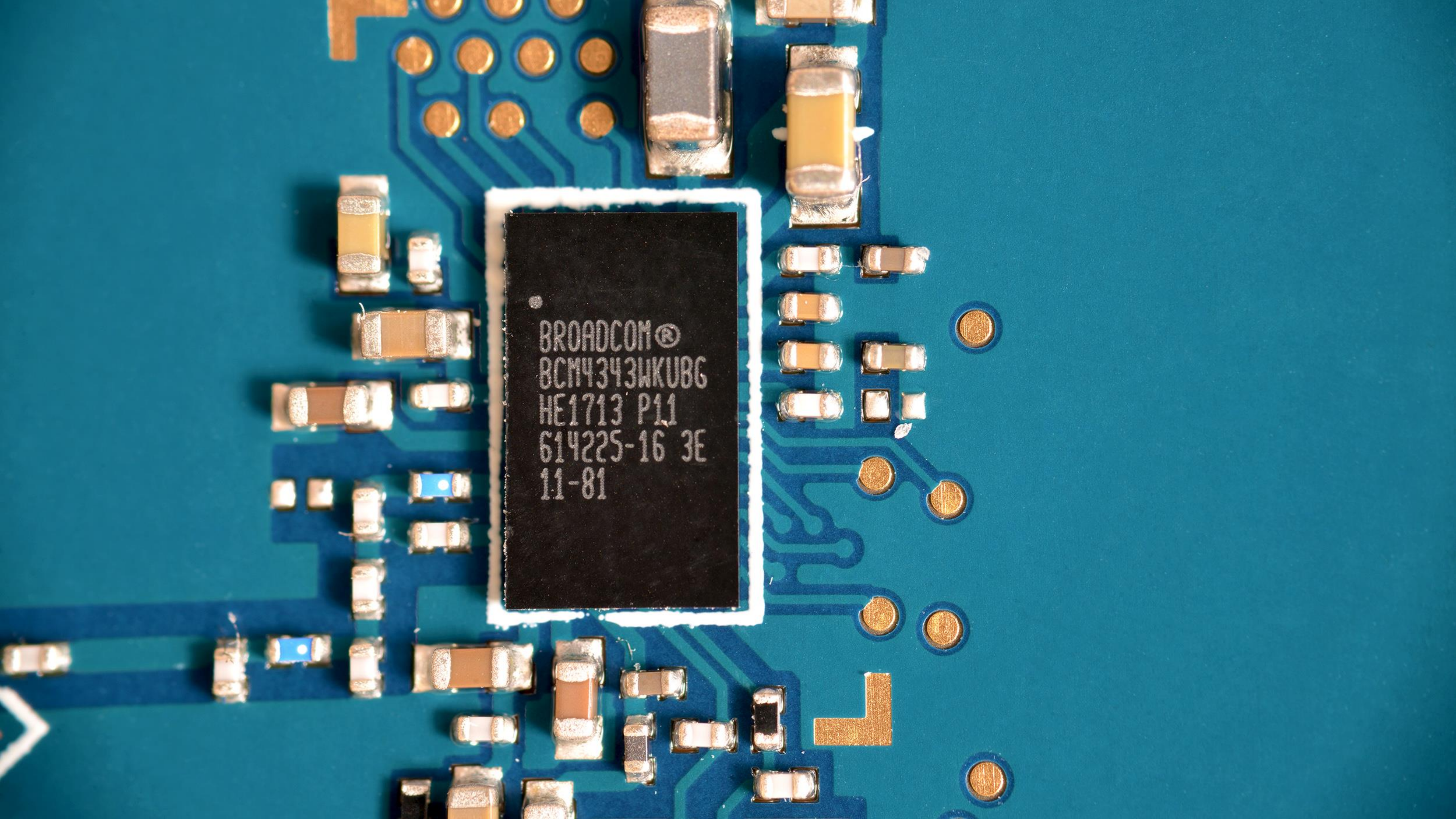
- Používajte aktualizovanú verziu aplikácie
- Uzavrite svoje meetingy pre verejnosť
- Opatrne s pozvánkami, najmä ak si vykopírujete URL
- Zapnite si „čakáreň (waiting room)“
- Vypnite niektoré features (chat, zdieľanie obrazovky atď)
- Ak je to potrebné, odstráňte používateľa, ktorý narúša meeting

Používate inú telekonferenčnú platformu?

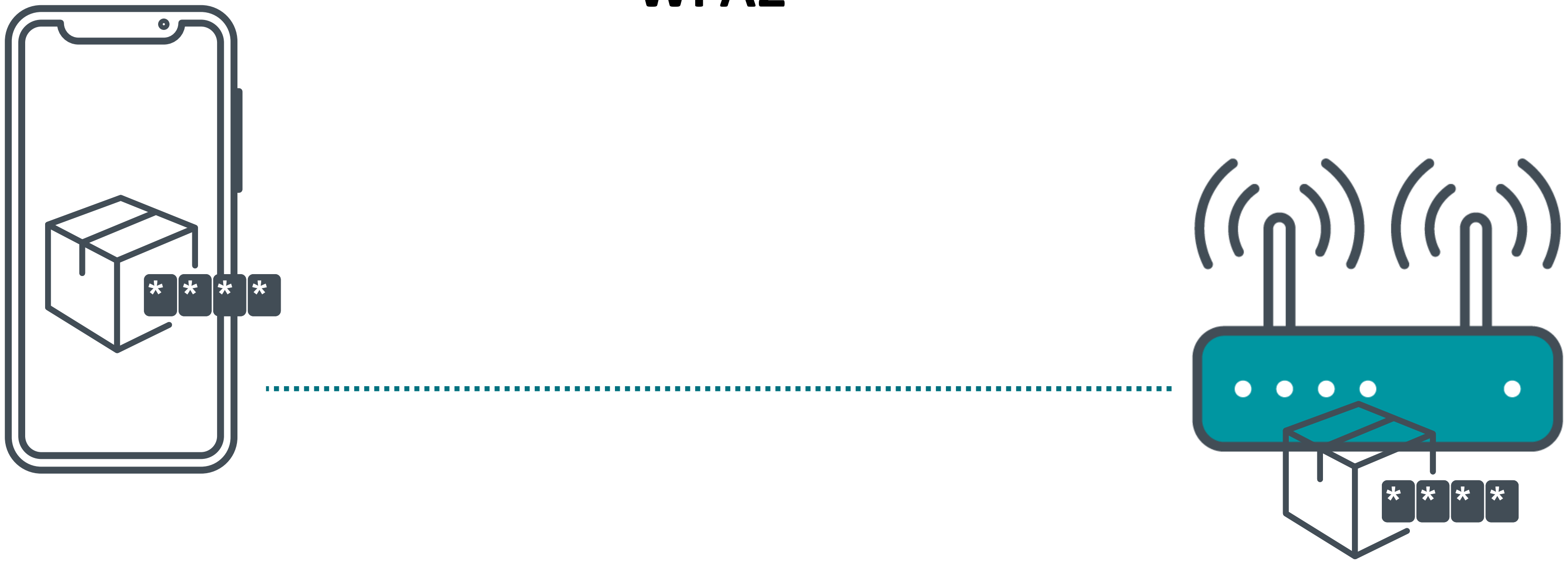
- Platí väčšina z už spomínaných pravidiel
- Skontrolujte si či platforma netrpí vážnymi zraniteľnosťami (MITRE alebo NIST)
- Používajte len podporovanú a aktualizovanú verziu aplikácie
- Uvedomte si riziká a hrozby (narušenie hovoru, únik dát atď.)

IoT

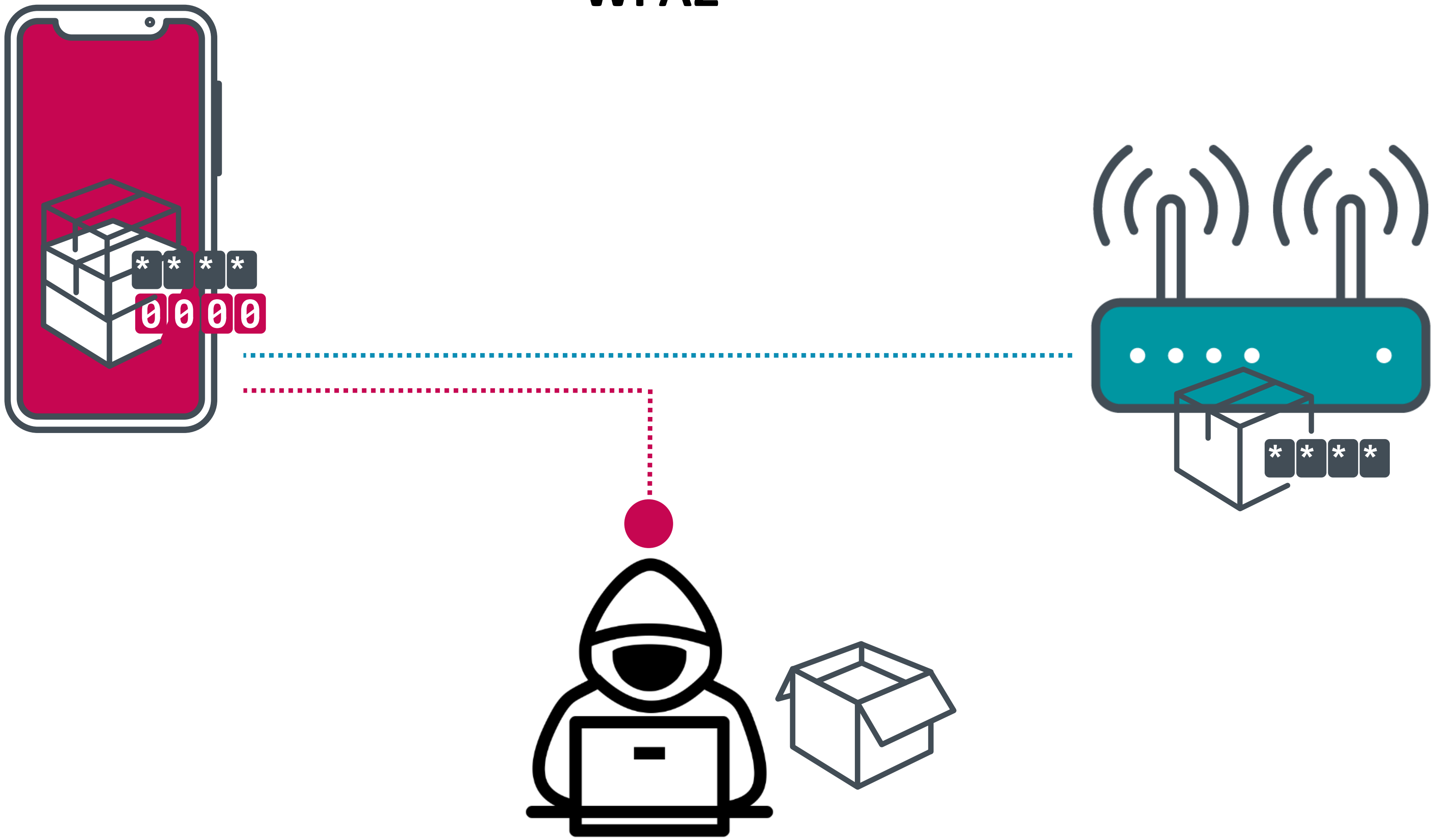
94V-0 T2H 1720
30-001931
REV 01
McNair
CE
IEC62133


BROADCOM®
BCM4343WKUBG
HE1713 P11
614225-16 3E
11-81

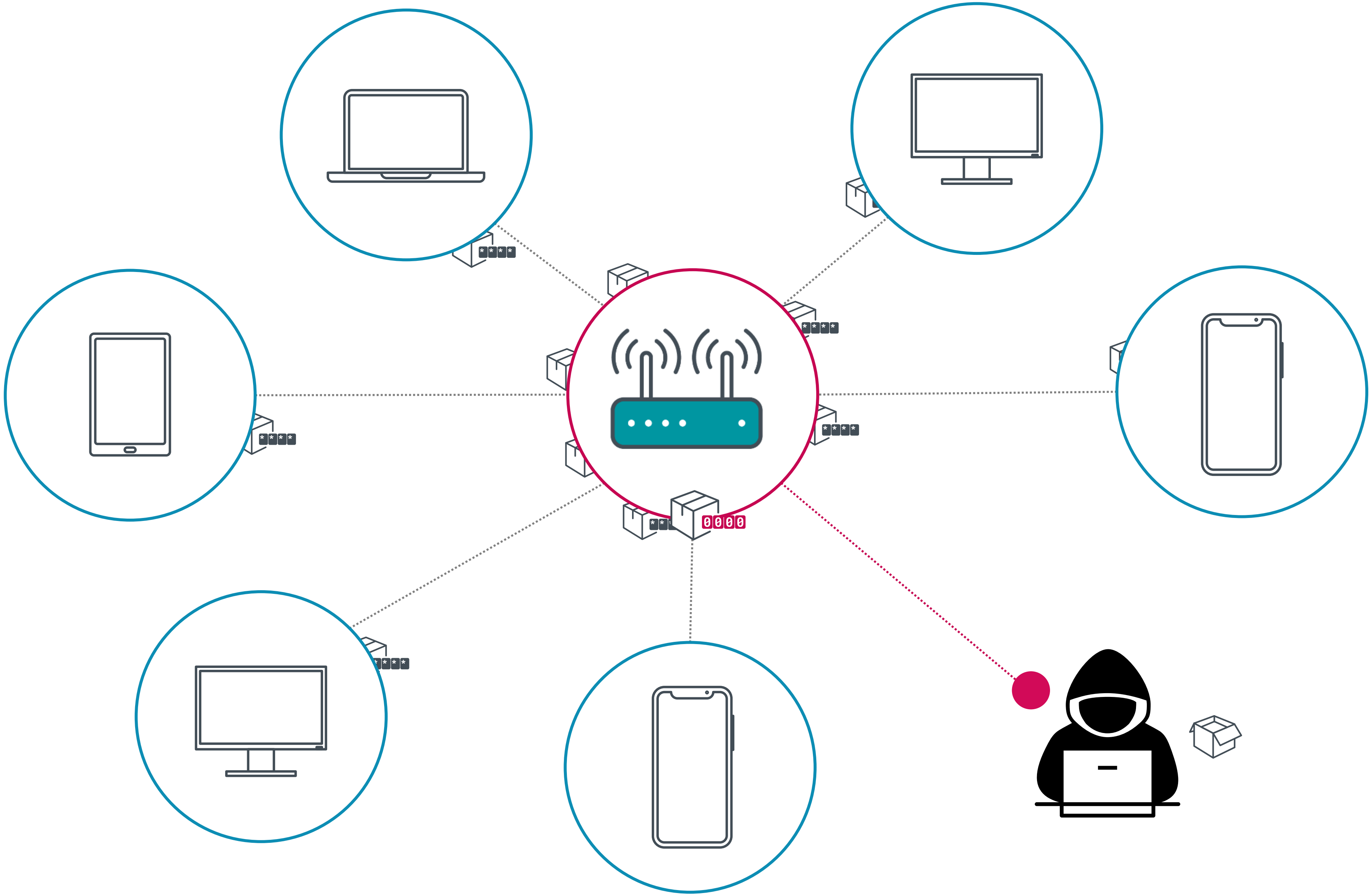
WPA2



WPA2



Zraniteľný Access Point vs. bezpečné zariadenia



Čoho všetkého sa týka Kr00k?

- Zariadení s Broadcom a Cypress FullMac Wi-Fi čipmi

- Zraniteľnosť potvrdená na:
  - ✓ Apple iPhone-och
  - ✓ Apple MacBook-och
  - ✓ Samsung Galaxy telefónoch
  - ✓ Google Nexus telefónoch
  - ✓ Xiaomi Redmi telefónoch
  - ✓ Raspberry Pi 3
  - ✓ Amazon Echo 2
  - ✓ Amazon Kindle 8
  - ✓ ASUS Wi-Fi routers
  - ✓ Huawei Wi-Fi routers

Čoho všetkého sa týka Kr00k?

- Zariadení s Broadcom a Cypress FullMac Wi-Fi čipmi

- Zraniteľnosť potvrdená na:
  - ✓ Apple iPhone-och
  - ✓ Apple MacBook-och
  - ✓ Samsung Galaxy telefónoch
  - ✓ Google Nexus telefónoch
  - ✓ Xiaomi Redmi telefónoch
  - ✓ Raspberry Pi 3
  - ✓ Amazon Echo 2
  - ✓ Amazon Kindle 8
  - ✓ ASUS Wi-Fi routers
  - ✓ Huawei Wi-Fi routers

Viac ako miliarda zariadení!

Takeaways

Čo môžu robiť firmy pre svoju ochranu?

- Zaručiť fyzickú bezpečnosť zariadení
- Zabezpečiť sieťové pripojenie
- Vynucovať unikátne a silné heslá, password manažérov a pridať ochranu ďalším faktorom
- Aktualizovať operačné systémy a softvér na všetkých zariadeniach
- Zvoliť bezpečné nástroje pre prácu z domu (na diaľku)
- Používať na všetkých zariadeniach spoľahlivé bezpečnostné riešenie s viacerými vrstvami
- Trénovať a informovať zamestnancov

Čo môžu robiť zamestnanci pre svoju ochranu?

- Zaručiť fyzickú bezpečnosť všetkých zariadení
- Aktualizovať domáce zariadenia vrátane routeru
- Používať unikátne a silné heslá
- Ostať doma a strážiť si zdravie