



Fake Online Coronavirus Map Delivers Well-known Malware

Date: March 10, 2020

EXECUTIVE SUMMARY:

A malicious website pretending to be the live map for Coronavirus COVID-19 Global Cases by Johns Hopkins University is circulating on the internet waiting for unwitting internet users to visit the website. Visiting the website infects the user with the AZORult trojan, an information stealing program which can exfiltrate a variety of sensitive data. It is likely being spread via infected email attachments, malicious online advertisements, and social engineering. Furthermore, anyone searching the internet for a Coronavirus map could unwittingly navigate to this malicious website.

Threat Details

A sample of the malware being deployed by "corona-virus-map[dot]com" was submitted and analyzed by and received an extremely malicious threat score of 100/100 with Anti-virus (AV) detection at 76%. This sample was labelled by Hybrid-Analysis as a Trojan.

Recommendations

End users should be warned about this cybersecurity risk and security teams should blacklist any indicators associated with this specific threat. IOCs and Analysis may be found here: <https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/>



Fake Online Coronavirus Map Delivers Well-known Malware

Date: March 10, 2020

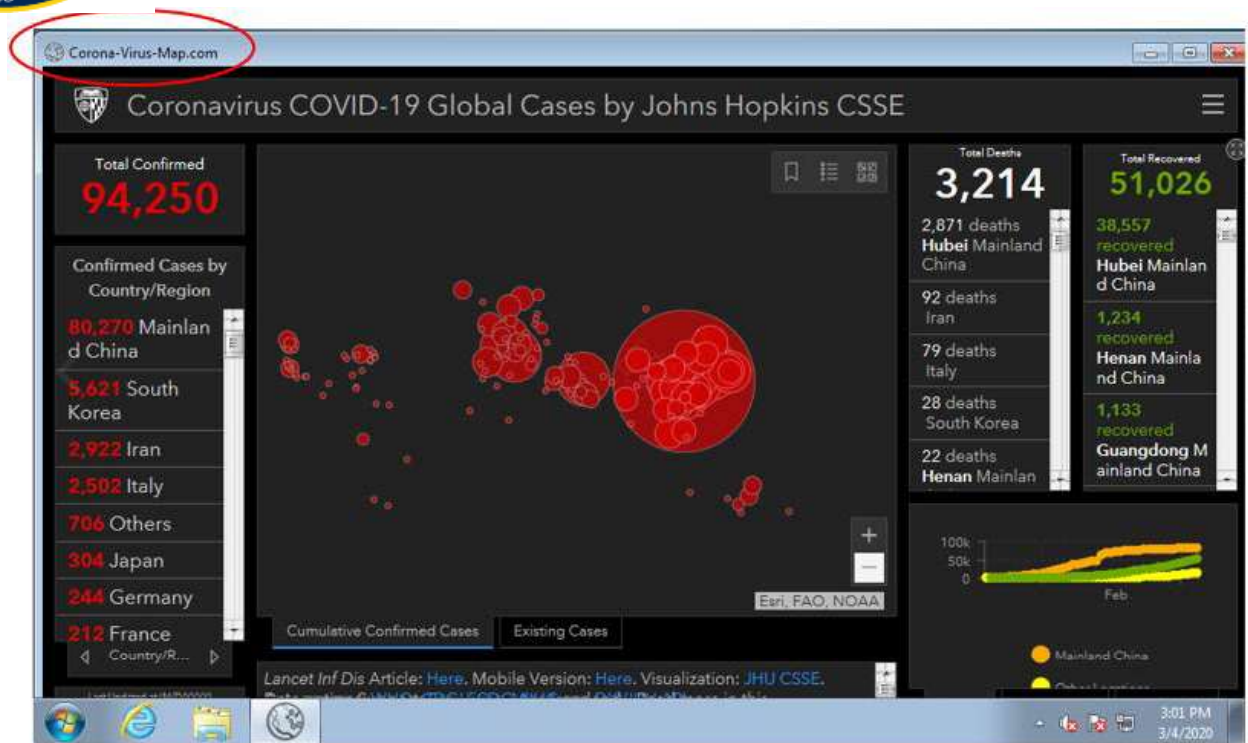


Figure 1. Screenshot of the malicious website "Corona-Virus-Map[dot]com" pretending to be a legitimate COVID-19 tracker.

corona-virus-map.com ▾ Translate this page
WordPress 5.0.2 – Ещё один сайт на WordPress
Добро пожаловать в WordPress. Это ваша первая запись. Отредактируйте или удалите ее,
затем начинайте создавать! Написано авторомadmin ...

Figure 2. Screenshot of a Google search for the page mentioned above.

Reference

Reason Labs. (March 9, 2020). COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report. Reasonsecurity.com. Accessed 10 March 2020 at <https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/>.

NEWS

Cyber experts step in as criminals seek to exploit Coronavirus fears

Experts at the NCSC have revealed phishing attacks exploiting worries over COVID-19



The public are being urged to follow online safety advice as evidence emerges that criminals are exploiting the Coronavirus online.

Experts from the National Cyber Security Centre have revealed a range of attacks being perpetrated online as cyber criminals seek to exploit COVID-19.

Techniques seen since the start of the year include bogus emails with links claiming to have important updates, which once clicked on lead to devices being infected.

These 'phishing' attempts have been seen in several countries and can lead to loss of money and sensitive data.

The NCSC, a part of GCHQ created to keep the UK safe online, is urging businesses and the public to consult its online guidance, including [how to spot and deal with suspicious emails](#) as well as [mitigate and defend against malware and ransomware](#).

In addition, in recent days the NCSC has taken measures to automatically discover and remove malicious sites which serve phishing and malware. These sites use COVID-19 and Coronavirus as a lure to make victims 'click the link'.

Paul Chichester, Director of Operations at the NCSC, said:

"We know that cyber criminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the Coronavirus outbreak.

"Our advice to the public is to follow our guidance, which includes everything from password advice to spotting suspect emails.

"In the event that someone does fall victim to a phishing attempt, they should look to report this to Action Fraud as soon as possible."

The NCSC has seen an increase in the registration of webpages relating to the Coronavirus suggesting that cyber criminals are likely to be taking advantage of the outbreak.

These attacks are versatile and can be conducted through various media, adapted to different sectors and monetised via multiple means, including ransomware, credential theft, bitcoin or fraud.

Continued global susceptibility to phishing will probably make this approach a

persistent and attractive technique for cyber criminals. Moreover, if the outbreak intensifies, it is highly likely that the volume of such attacks will rise.

There are numerous examples of cyber attacks worldwide since the Coronavirus outbreak.

On 16 February, the World Health Organisation (WHO) [warned of fraudulent emails sent by criminals posing as the WHO](#). This followed a warning from the US Federal Trade Commission about scammers spreading phishing 'clickbait' via email and social media, as well as creating fraudulent websites to sell fake antiviral equipment.

Cyber criminals have also impersonated the US Center for Disease Control (CDC), creating domain names similar to the CDC's web address to request passwords and even bitcoin donations to fund a fake vaccine.

In January, attackers spread the Emotet banking trojan in Japan by posing as a state welfare provider to distribute infected Word documents. Similar operations have been observed in Indonesia, the US and Italy, with attackers attempting to spread the Lokibot infostealer, Remcos RAT and other malware.

Individuals in the UK have also been targeted by Coronavirus-themed phishing emails with infected attachments containing fictitious 'safety measures.' [According to Proofpoint researchers](#), such attacks have recently become more targeted, with greater numbers focusing on specific sectors like shipping, transport or retail to increase the likelihood of success.

PUBLISHED

16 March 2020

WRITTEN FOR 

[Individuals & families](#)

NEWS

NCSC issues guidance as home working increases in response to COVID-19

Advice to help organisations manage the cyber security challenges of increased home working.



Organisations are being urged to follow cyber security best practice [guidance to help prepare for an increase in home and remote working](#) in the wake of the coronavirus (COVID-19) outbreak.

The National Cyber Security Centre (NCSC) has today published advice for UK companies to reduce the risk of cyber attack on deployed devices including

laptops, mobiles and tablets, and tips to help staff spot typical signs of phishing scams.

Working from home is new for a lot of organisations and employees. Even if home working has been supported for some time, there may suddenly be more people working from home than usual, some of whom may not have done it before.

The NCSC has outlined recommended steps for organisations in:

- Preparing for home working
- Setting up new accounts and accesses
- Controlling access to corporate systems
- Helping staff to look after devices
- Reducing the risk from removable media

Within the guidance there is advice on dealing with suspicious emails, as [evidence emerges that criminals are exploiting the coronavirus online](#) by sending phishing emails that try and trick users into clicking on a bad link. If clicked, these links could lead to malware infection and loss of data like passwords. The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

The guidance offers advice on spotting those emails, as well as on how to respond in the event of falling victim to a scam.

For official information about coronavirus, please refer to trusted resources such as the [Public Health England](#) or [NHS](#) websites.

PUBLISHED

17 March 2020

NEWS TYPE

General news

WRITTEN FOR 

[Small & medium sized organisations](#)

[Large organisations](#)

[Public sector](#)

[Cyber security professionals](#)

BYOD

Bring Your Own Device

Guidance for private and public sector organisations considering a BYOD approach.



Limit the information shared by devices

Staff are used to sharing their information with other users and in the cloud. The automated backup of device data to cloud based accounts can lead to business data being divulged.



Create effective BYOD policy

Ensure that personally-owned devices are only able to access business data that you are willing to share with authorised staff.



Consider using technical controls

Container applications and technical services such as Mobile Device Management can help you remotely manage personally-owned devices, but they can impact the usability of the device.



Plan for security incidents

When incidents occur, act quickly to limit losses. Could you remotely wipe sensitive data from a personally-owned device if it was lost or stolen?



Consider alternative ownership models

Restricted devices may not appeal to some users, so consider giving staff a choice of approved devices which are purchased and controlled by your organisation.



Encourage staff agreement

Communicate your BYOD policy through staff training so they understand their responsibilities when using personally-owned devices for work purposes.



Anticipate increased device support

Your services may need to be accessed by different types of device, so ensure you have the IT support capability and expertise to manage a growing range of devices.



Understand the legal issues

The legal responsibility for protecting other people's personal information is with the data controller, not the device owner.



Ransomware

Prevention & recovery

Following this advice can reduce the likelihood of you becoming a victim of ransomware. Ransomware makes your data or computers unusable and asks you to make a payment to release it. If your computer is already infected with ransomware, we've included some useful recovery steps below. For more information, please refer to www.ncsc.gov.uk/ransomware.

What is ransomware?

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer).

If your computer is infected with ransomware, the computer itself may become **locked**, or the data on it might be **stolen**, **deleted** or **encrypted**.


Normally you're asked to make a payment (the ransom), in order to 'unlock' your computer (or to access your data).

However, even if you pay the ransom, there is **no guarantee** that you will get access to your computer, or your files. This is one of the reasons why it's important to always have a recent backup of your most important files and data.

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.



 **Make regular backups** of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.



Make sure the device containing your backup (such as an external hard drive or a USB stick) **is not permanently connected** to your computer.



Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.



Keep your operating system and apps up to date. Apply software updates promptly, they contain patches that keep your device secure, including protection from ransomware and other types of virus.



Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.



Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:



Open your antivirus (AV) software, **and run a full scan**. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device.



Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.



If you receive a phone call offering help to clean up your computer, **hang up immediately** (this is a common scam).



Anyone who thinks they may have been subject to a ransomware attack should **contact Action Fraud** (www.actionfraud.police.uk). Organisations should call 0300 123 2040. In Scotland, contact the police by dialing 101.

Should I pay the ransom?

The NCSC encourages you **not** to pay the ransom. If you do:



- there is no guarantee that you will get access to your data or computer
- your computer will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in the future

BLOG POST

Updating our malware & ransomware guidance

Here's what's changed in the NCSC's guidance on mitigating malware and ransomware.

Emma W



We recently updated our mitigating malware guidance; it's now called **Mitigating malware and ransomware attacks**. We also took the opportunity to retire our standalone ransomware guidance. This blog post explains what we changed, and why we did it.

Two becomes one...

Having two separate pieces of guidance was confusing for some of our customers. Most of the **ransomware** content was the same in both pieces of guidance, but the **malware** guidance was slightly more up-to-date. So we have tried to make things easier by providing a single piece of guidance, with all the most up-to-date advice in one place.

New content on offline backups

We improved the guidance by emphasising *offline* backups as a defence against ransomware. We've seen a number of ransomware incidents lately where the victims had backed up their essential data (which is great), but all the backups were online at the time of the incident (not so great). It meant the backups were also encrypted and ransomed together with the rest of the victim's data. We've previously published a blog post [recommending offline backups](#), but [recent incidents](#) suggest we need to emphasise the importance of this in our guidance as well.

Tidying up and sweeping down

While we were updating the guidance, we took the opportunity to remove some of the more detailed technical content, as feedback showed that customers tend to find these parts less useful. The new guidance is not only shorter, but hopefully more relevant.

Finding information in a hurry

Some people have already pointed out that since ransomware is a type of malware, saying 'malware AND ransomware attacks' isn't 100% accurate.

However, not everyone who visits our website knows that. Furthermore, they might well search for the term 'ransomware' (rather than 'malware') when they're in the grip of a live ransomware incident. We want to be as helpful as possible to the people who need our guidance in a hurry. The best cyber security advice in the world is useless if nobody can find it.

For the same reason, we used 'attacks' rather than 'infections', 'incidents' or 'compromises' – as we know this is by far the most popular search term. These technical trade-offs are sometimes necessary, because the NCSC needs to make sure the language used in its guidance matches what's being used in the real world.

Do you like the new guidance? Let us know! Tweet us [@NCSC](#) or [email the enquiries team](#).

Emma W

Head of Guidance, NCSC communications



WRITTEN BY

[Emma W](#)

PUBLISHED

26 February 2020

WRITTEN FOR ⓘ

[Public sector](#)

[Cyber security professionals](#)

[Large organisations](#)

PART OF BLOG

[NCSC publications](#)