Cyber Threat Intelligence Alert

Hackers Continue to Exploit the COVID-19 Pandemic in Malicious Campaigns

TLP: WHITE

March 2020

SenseCy
A VERINT. Company

Powered by LUMINAR cis.verint.com/luminar

1.1 19-03-2020-001: Hackers Continue to Exploit the COVID-19 Pandemic in Malicious Campaigns

Threat Level:	High
Threat Vector:	Malware
Threat Actor:	Nation-State Actors; Cybercriminals
Targeted Assets:	End Users
Information Source:	OSINT
Credibility Score:	B2 - Credible

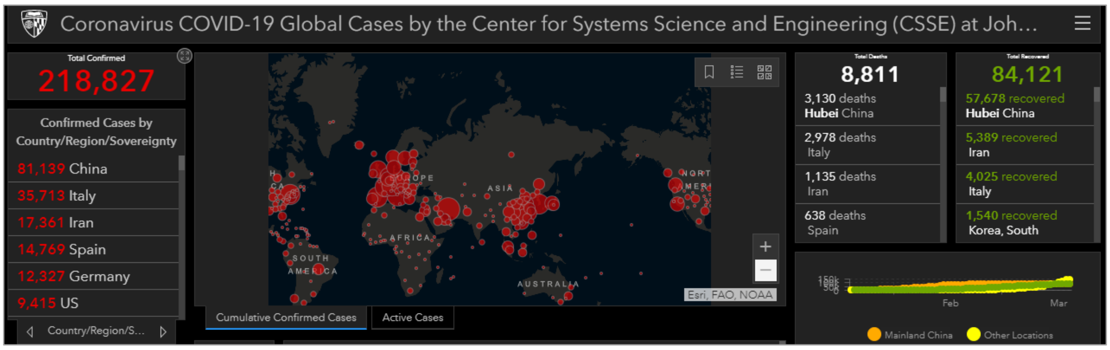
Recommendations:

+ Implement the technical IOCs attached to this report in your security systems.

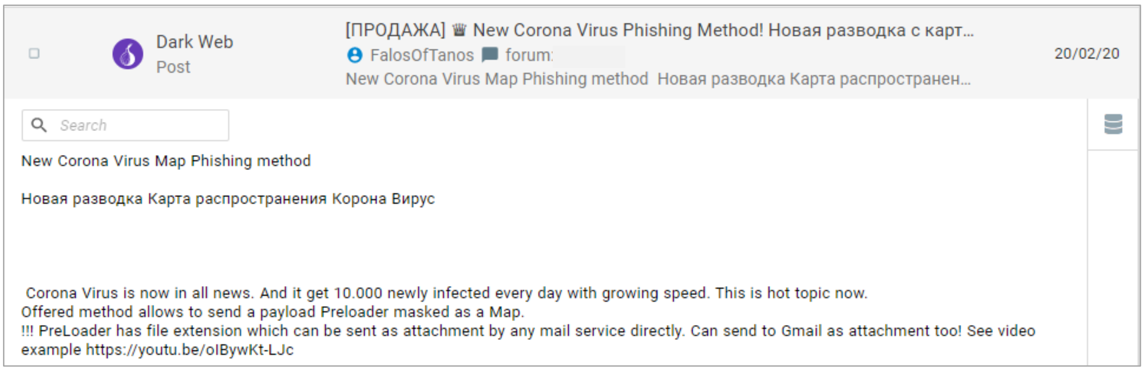
As the Coronavirus (COVID-19) epidemic continues to spread throughout the world in recent weeks, additional malicious campaigns were identified exploiting the recent panic and the constant search for information and updates on the virus in order to spread various types of malware.

1.1.1 Cybercrime Threat Actors

Firstly, security researchers have identified Russian cybercriminals selling malicious versions of the highly popular interactive map of COVID-19 cases around the world, created by Johns Hopkins Coronavirus Resource Center. In fact, these versions include infostealer malware, intended on stealing information from its victims' computers.[1]



[1] https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/



Dark Web
Post

[ПРОДАЖА] ♛ New Corona Virus Phishing Method! Новая разводка с карт...
FalosOfTanos forum:
New Corona Virus Map Phishing method Новая разводка Карта распространен...

20/02/20

Search

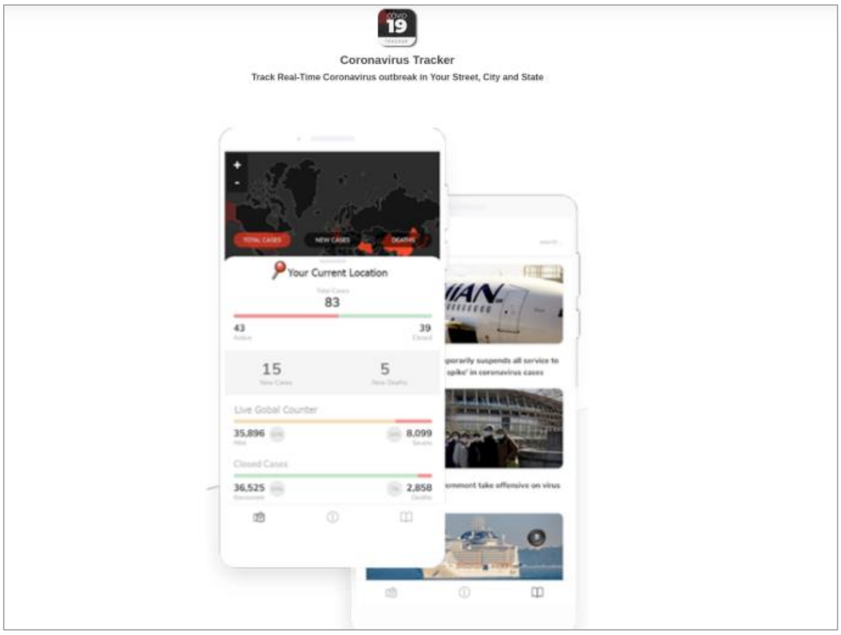
New Corona Virus Map Phishing method

Новая разводка Карта распространения Корона Вирус

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 https://youtu.be/oIBywKt-LJc

The Johns Hopkins Coronavirus Resource Center' map (above) and the sells offer of the malicious map on a Russian Dark Web forum (below, source: Verint Luminar)

In addition, a new malicious domain was discovered, coronavirusapp[.]site, which is offering to download an Android app that tracks the spread of the virus and also includes statistical data. However, the application is actually poisoned with *CovidLock*, a ransomware that changes the password used to unlock the device, thus denying the victims access to their phones. The victims are required to pay a ransom fee of US$ 100 in Bitcoin, or else, according to the ransom note, their contacts, pictures, videos and device's memory will all be erased.[2]

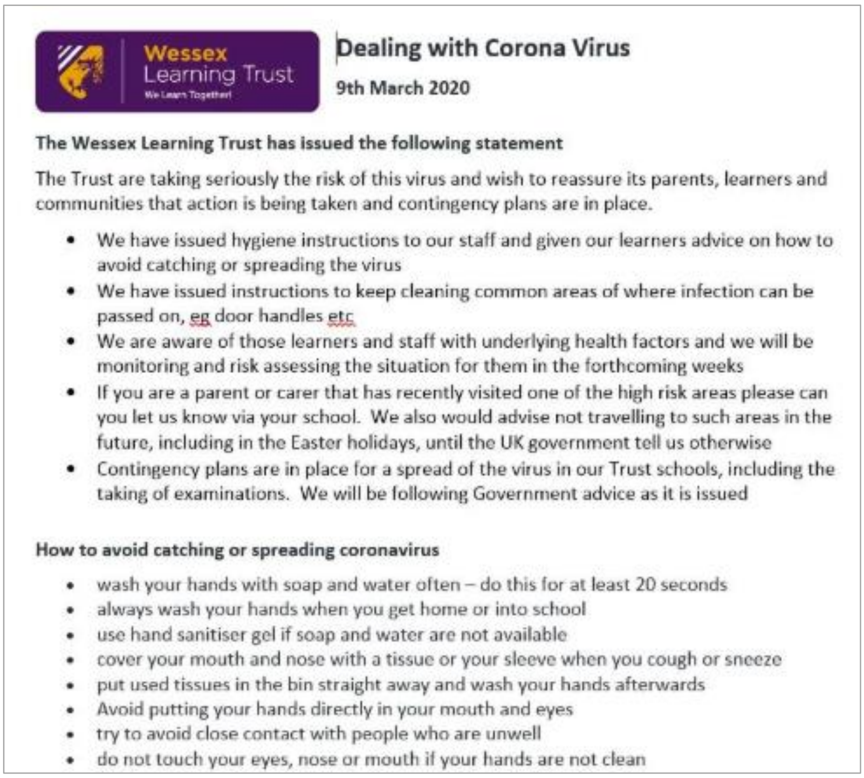


Screenshot of the coronavirusapp[.]site domain. Source: DomainTools

Security researchers have also discovered a new backdoor distributed in RAR format. The file includes an executable masquerading as a Microsoft Word file with information on COVID-19, intended to install the rest of the malware on the victim's computer. The researchers estimate that file is being distributed via phishing emails.[3]

[2] https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware

[3] https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2-communication/



Dealing with Corona Virus

9th March 2020

The Wessex Learning Trust has issued the following statement

The Trust are taking seriously the risk of this virus and wish to reassure its parents, learners and communities that action is being taken and contingency plans are in place.

- We have issued hygiene instructions to our staff and given our learners advice on how to avoid catching or spreading the virus
- We have issued instructions to keep cleaning common areas of where infection can be passed on, eg door handles etc
- We are aware of those learners and staff with underlying health factors and we will be monitoring and risk assessing the situation for them in the forthcoming weeks
- If you are a parent or carer that has recently visited one of the high risk areas please can you let us know via your school. We also would advise not travelling to such areas in the future, including in the Easter holidays, until the UK government tell us otherwise
- Contingency plans are in place for a spread of the virus in our Trust schools, including the taking of examinations. We will be following Government advice as it is issued

How to avoid catching or spreading coronavirus

- wash your hands with soap and water often – do this for at least 20 seconds
- always wash your hands when you get home or into school
- use hand sanitiser gel if soap and water are not available
- cover your mouth and nose with a tissue or your sleeve when you cough or sneeze
- put used tissues in the bin straight away and wash your hands afterwards
- Avoid putting your hands directly in your mouth and eyes
- try to avoid close contact with people who are unwell
- do not touch your eyes, nose or mouth if your hands are not clean

The Word file presented to the victim as a distraction while the malware is executed

Moreover, a new ransomware called *CoronaVirus* was recently identified being distributed through a fake website of WiseCleaner, a service offering system utilities for Windows OS. Download files on this malicious site act as downloaders for both the *CoronaVirus* ransomware and a stealer called *Kpot*. The ransomware is called *CoronaVirus* because when it encrypts the files, it changes their names to include the attackers' email address, coronaVi2022@protonmail.ch, and the ransom note is saved in a text file called CoronaVirus.txt.[4]

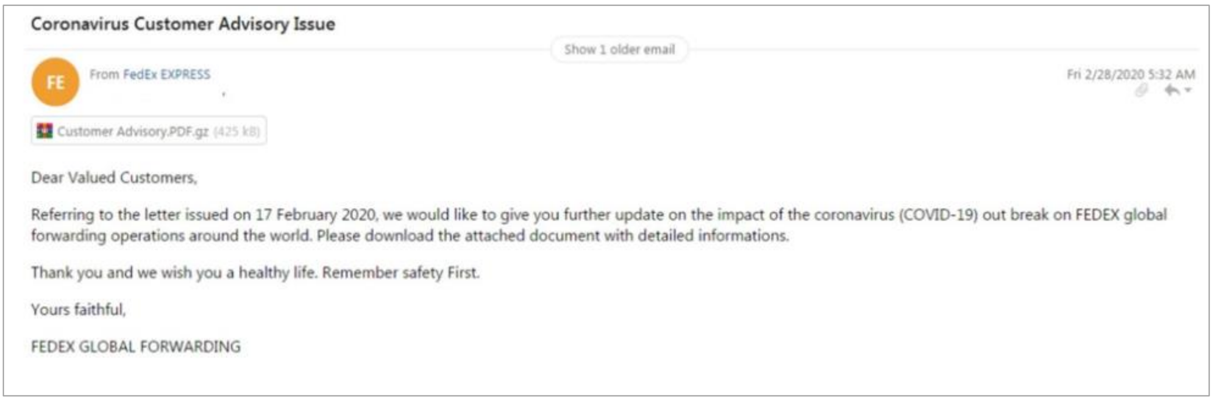
Additional campaigns utilize phishing emails with malicious attachments that supposedly include information and updates on Coronavirus, but in fact download different malware to the victims' computers, including a banking Trojan called *TrickBot*,[5] a Stealer called *LokiBot*[6] and a Stealer called *FormBook*.[7]

[4] https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/

[5] https://news.sophos.com/en-us/2020/03/04/trickbot-campaign-targets-coronavirus-fears-in-italy/

[6] https://www.fortinet.com/blog/threat-research/attackers-taking-advantage-of-the-coronavirus-covid-19-media-frenzy.html

[7] https://www.bleepingcomputer.com/news/security/data-stealing-formbook-malware-preys-on-coronavirus-fears/



Coronavirus Customer Advisory Issue

From FedEx EXPRESS

Fri 2/28/2020 5:32 AM

Customer Advisory.PDF.gz (425 kB)

Dear Valued Customers,

Referring to the letter issued on 17 February 2020, we would like to give you further update on the impact of the coronavirus (COVID-19) out break on FEDEX global forwarding operations around the world. Please download the attached document with detailed informations.

Thank you and we wish you a healthy life. Remember safety First.

Yours faithful,

FEDEX GLOBAL FORWARDING

Coronavirus-themed phishing email impersonating FedEx to infect the recipient with LokiBot. Source: Fortinet.

1.1.2 State-Sponsored Actors

Security researchers have also identified state-sponsored threat actors exploiting the COVID-19 panic to promote their interests and carry out attack campaigns. In early March 2020, researchers discovered a campaign launched by a Chinese APT group against targets in Vietnam, using emails with a malicious RAR file that ostensibly included a message from Vietnam's prime minister on Coronavirus.[8] In reality, the file downloaded a backdoor malware to the victims' computers. Another Chinese APT group attacked targets in Mongolia's government using malicious documents that supposedly contain new information on the virus.[9]

Additionally, another APT group originating from North Korea has sent phishing messages to South Korean officials that ostensibly included a document detailing the reaction of the country to the pandemic. In fact, the document contained a malware called *BabyShark*, associated with a North Korean APT group.[10]

Lastly, security researchers identified another campaign by a Russian APT Group that sent malicious files, seemingly including updates on Coronavirus, in order to distribute a backdoor malware to targets in Ukraine. The Russian hackers pretended to be from the Center for Public Health of the Ministry of Health of Ukraine so that they could deliver emails containing these malicious files.[11]

In conclusion, cybercriminals and state-sponsored threat actors are using the panic resulting from the Coronavirus epidemic for phishing purposes and malware distribution. As the virus continues to spread across the world, preoccupying the global agenda, it can be estimated we will witness more campaigns exploiting the crisis.

[8] https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/
https://blog.vincss.net/2020/03/re012-phan-tich-ma-doc-loi-dung-dich-COVID-19-de-phat-tan-gia-mao-chi-thi-cua-thu-tuong-Nguyen-Xuan-Phuc.html

[9] https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

[10] https://twitter.com/issuemakerslab/status/1233010155018604545

[11] https://twitter.com/RedDrip7/status/1230683740508000256
https://mp.weixin.qq.com/s/o6KC0k43AuOY5F8FKGbmMg

1.1.3 Best Practices for Secure Remote Working

On account of the global situation related to COVID-19, organizations worldwide have directed their employees to work remotely from home, which may leverage the security risks to the employee and the organization. Among these risks are:

- Unsecure Wi-Fi connection
- Unsecure remote connection to organization network
- Outdated security tools
- Attacks by threat actors seeking to exploit the COVID-19 pandemic and take advantage of the sense of anxiety in society

Based on the above, we recommend the following practices for ensuring employees work remotely in a secure way:

- Allow remote access to the organization's network with two-factor authentication only.
- Ensure remote sessions are automatically timed out after a certain period of inactivity, and require re-authentication.

Guide employees to:

- strengthen the security of their Wi-Fi connection by setting a password for their router at home
- use a VPN so their connection is secured and encrypted
- ensure their security tools (anti-virus, firewall) are fully updated
- back up important files on a regular basis.
- be extra vigilant regarding any COVID-19-related communication from supposedly internal, or external sources, especially those that encourage the user to take action, such as clicking on a link, opening an attachment, downloading a document or an app, or visiting a website.

Implement the technical IOCs attached to this report in your security systems.

Legend

Threat Level

Cyber threat levels are rated in accordance with the Multi-State Information Analysis Center (MS-ISAC) threat-level system:

- **Severe**. Specific risk of hacking, virus, or other malicious activity.
- **High**. High risk of malicious activity that targets or compromises core infrastructure.
- **Elevated**. Significant risk due to increased malicious activity that compromises systems or diminishes service.
- **Guarded**. General risk of increased hacking, virus or other malicious activity.
- **Low**. No unusual activity exists beyond normal concern for malicious activity.

Admiralty Code – Source Reliability and Information Credibility

Source Reliability

Information Credibility	A	B	C	D	E	F
1	🟩 A1	🟩 B1	🟩 C1	🟩 D1	🟩 E1	🟨 F1
2	🟩 A2	🟩 B2	🟩 C2	🟩 D2	🟨 E2	🟨 F2
3	🟩 A3	🟩 B3	🟨 C3	🟨 D3	🟥 E3	🟨 F3
4	🟨 A4	🟨 B4	🟨 C4	🟥 D4	🟥 E4	🟥 F4
5	🟨 A5	🟨 B5	🟥 C5	🟥 D5	🟥 E5	🟥 F5
6	🟨 A6	🟨 B6	🟥 C6	🟥 D6	🟥 E6	🟨 F6

🟩 Credible
🟨 Uncertain
🟥 Non-Credible

Traffic Light Protocol

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs the following colors to indicate expected sharing boundaries to be applied by the recipient(s).

- **Red**. Not for disclosure, restricted to participants only.
- **Amber**. Limited disclosure, restricted to participants' organizations.
- **Green**. Limited disclosure, restricted to the community.
- **White**. Disclosure is forbidden.

Disclaimer and Limitation of Liability

Copyright and License of Product

This report (the "Product") is the property of SenseCy (part of Verint's group), and is protected by Israel and international copyright law and conventions. User acknowledges that access to the Product is limited to the License terms set forth herein and any expansion must be in writing. The granting of the License to access and use the Product is conditioned on User's agreement not to disclose, copy, disseminate, redistribute, or publish the Product, or any portion of or excerpts thereof to any other party.

All materials included in this report were collected by using legal Open Source Intelligence methodologies and supporting technologies. This report does not include interrogation of any specific entity and/or individual.

User shall have the right to use the Product solely for its own internal information purposes. Reproduction of the Product in any form or by any means is forbidden without SenseCy's written permission.

User agrees to maintain all copyright, trademark and other notices contained in the Product. User agrees that it shall not use SenseCy's name or any excerpts from the Product in the promotion of its products or services.

Disclaimer of Warranties

SenseCy does not make any warranties, express or implied, including, without limitation, those of merchantability and fitness for a particular purpose, with respect to the Product. Although SenseCy takes reasonable steps to screen the Product for infection by viruses, worms, Trojan horses or other code manifesting contaminating or destructive properties before making the Product available, SenseCy cannot guarantee that the Product will be free of infection. SenseCy does not make any warranties, express or implied, of whatsoever nature with respect to the Product or to the accuracy of any conclusions set out in the Product.

Accuracy of Information

The information contained in the Product has been obtained from sources believed to be reliable and are provided by SenseCy on an "as is" basis. To the full extent permissible by applicable law, SenseCy disclaims all warranties, express or implied, of whatsoever nature including, but not limited to any warranties as to the accuracy, completeness, quality or adequacy of any such information, any conclusions set out in the Product and any translations in the Product. The reader assumes sole responsibility for the selection of the Product to achieve its intended results. The opinions expressed in the Product are subject to change at any time without notice.

Limitation of Liability

To the extent permitted under applicable law, in no event will SenseCy be liable in any way for:

1. damages of any kind, including without limitation, direct, incidental punitive, special or consequential damages (including, but not limited to, damages for lost profits, business interruption and loss of programs or information) arising out of the use of or inability to use the Product, or any information provided in the Product, regardless of whether or not SenseCy has been advised of the possibility of such damages;
2. any claim attributable to errors, omissions or other inaccuracies in the Product or interpretations thereof; and
3. actions taken or not taken by any person or entity as a result of the review by such person or entity of the Product or information contained therein or as a result of the interpretation of the Product or information contained therein by such person or entity.

Indemnification

User agrees to indemnify, defend and hold harmless SenseCy, its affiliates, licensors, and their respective officers, directors, employees and agents from and against all losses, expenses, damages and costs, including reasonable attorneys' fees, arising out of the use of the Product by User or User's account.

Third Party Rights

The provisions regarding Disclaimer of Warranty, Limitation of Liability and Indemnification are for the benefit of SenseCy, and its licensors, employees and agents. Each shall have the right to assert and enforce those provisions against a User.

General Provisions

Any provision in any memorandum received by SenseCy in connection with the Product which is inconsistent with, or adds to, the provisions of this Agreement is void. Neither the parties' course of conduct or trade practice will modify the terms of this Agreement. If any provision of this Agreement is determined by a court of competent jurisdiction to be invalid, all other terms and conditions shall remain in full force and effect.

Governing Law

This Agreement and the resolution of any dispute arising hereunder shall all be governed and construed in accordance with the laws of the state of Israel, without regard to its conflicts of law principles. User consents to the jurisdiction of the courts of Tel-Aviv.