CERT-EU

Coronavirus – Cyber exploitation

Threat Alert - Date: 06/03/2020 - Version: 1.0
TLP:WHITE

	Category	Type	Threat Level	Domain	Sector	Confidence
FOR ACTION	Cybercrime Cyberwar	Scam, Disinformation, Fake news	Low	World	Any	A1

Key Points

- Heightened public interest on the coronavirus spurs cybercriminal and disinformation operations.
- At least six different pieces of malware have been distributed using fraudulent coronavirus-themed emails in several campaigns worldwide.
- At least two likely state-sponsored information operations have been reported.

Summary

Due to the global coronavirus outbreak (officially COVID-19) there has been heightened public interest on getting the latest updates on the extent of its spread, as well as infection and protection methods. Cybercriminals are exploiting this, using coronavirus themed emails to lure victims to online scams or as vehicles for malware delivery.

Additionally, in the last two weeks it appears that the interest, even fear, generated around the coronavirus is used to spread disinformation for political purposes:

- In Ukraine it has led on February 20, 2020 to public protests and clashes as incorrect information pertaining to the number of victims was spread on the same day that quarantined persons stranded in other countries were repatriated[1].
- According to US officials[2], thousands of Russian-linked social media accounts have launched a coordinated effort to spread misinformation and alarm about coronavirus, disrupting global efforts to fight the epidemic.

Overall the main occurring themes of the phishing emails have been:

- Disease centres alerts
- Information on the spread of coronavirus
- Expert protection advice
- Analysis on impacts to economy sectors or to other areas
- Offers to invest in “cures”, vaccines, wonder medicine, protection products.
- “Interesting” facts/videos about the disease.
- Strong statements on the “origin” of the virus, indicating human responsibility of certain countries
- Misleading stories on the number of victims, how a government is handling the situation, etc., aiming to spread fear and discontent.

The main techniques employed to lure victims have been:

- Phishing mails,
- Infected attachments (MS-Word, PDF, image files, etc.),
- Fraudulent links,
- Fake websites, including one impersonating the World Health Organisation (WHO),
- Fake downloads, asking for the user email credentials,
- Downloads carrying malware.

[1] https://www.buzzfeednews.com/article/christopherm51/coronavirus-ukraine-china
[2] https://www.theguardian.com/world/2020/feb/22/coronavirus-russia-disinformation-campaign-us-officials

The main pieces of malware observed have been:

Malware family	Details
Emotet	The Emotet trojan (ATT&CK S0367) is frequently used as a delivery method for other cybercrime malware including ransomware (for additional information, please see TA 2020-004)
Azorult	The Azorult is an information stealer (ATT&CK S0344)
Kiron	A Brazilian banking trojan
Lokibot	Information stealer
Remcos	Remote Access Trojan (RAT) (ATT&CK S0332)
Trickbot	Banking trojan
Unspecified	Additional, unnamed pieces of malware aiming to collect and exfiltrate victim information.

Comment

As the coronavirus situation develops, responsible EU authorities are also responding with useful information, warnings, etc. EU-I staff are going to receive emails from legitimate sources, including regular announcements by EU official channels. It is also almost certain that there will be continuous but not necessarily targeted attempts against EU-I by threat actors making use of the public concern of the coronavirus situation. EU-I staff should follow best practices concerning trusting information on received emails. EU Institutions responsible for disseminating relevant information will use trusted channels, including websites with verified digital certificates.

Please see actionable information on the following page.

Actionable information

Timeline

Examples of recent malicious cyber campaigns around COVID-19

Date	Type	Country	Impersonated entity	Malware	Event/Email theme
End of January 2020	Phishing, Malware	Japan	Public health centres	Emotet	Emails attachments supposedly providing information on the prevention measures.
Beginning of February 2020	Phishing, Malware	US, UK	US Centres for Disease Control and Prevention (CDC) Virologists		At least two phishing campaigns: CDC Alerts, with updated lists of infection cases around the recipient's location. Protection advice in an attached (malicious) PDF file.
February 4, 2020	Phishing, Malware		Ministry of Health of China	Lokibot	Official Emergency Regulations regarding the coronavirus.
February 5, 2020	Phishing, Credential harvesting	World	WHO		Safety measures information, linking to a page in which the users were lured to supply their email username and password in order to get information.
February 10, 2020	Warning	US			The US Federal Trade Commission (FTC) issued a warning[3] about all the possible ways the coronavirus issue could be used to scam consumers.
February 12, 2020	Phishing, Malware			Azorult	Campaign supposedly informing about global disruptions in shipping due to the coronavirus outbreak.
February 13, 2020	Phishing, Malware	Brazil		Kiron	Website in which videos of fast-track hospital construction in China were supposedly available.
February 17, 2020	Warning	World			WHO issued a cybersecurity warning[4].
Mid-February 2020	Scam	World	Hong Kong Department of Health		Emails asking for donations.
February 20, 2020	Phishing, Malware	Ukraine	Centre for Public Health of the Ministry of Health of Ukraine		A coronavirus-themed Microsoft Office document, containing malicious macros and dropping an information gathering backdoor.
February 20, 2020	Dis-information	Ukraine	Ukraine's Health Ministry		False information that there were five cases of coronavirus in the country, Interestingly the email had been sent to real Ministry of Health contact lists. The Security Service of Ukraine (SBU) released a statement that the email had originated from outside Ukraine. Later, more fake news reported that medical staff from a hospital were fleeing the facility.
February 20, 2020	Malicious tool advertised			Malware	A pre-loader, accompanied by a purported real-time interactive map of infections to assist the believability of phishing campaign.
February 27, 2020	Phishing, Malware			Remcos	Protection advice by the file (probably delivered as attachment) CoronaVirusSafetyMeasures_pdf.exe.
March 2, 2020	Fraud	US			Amazon.com reported taking down more than 1 million products due to overcharging or false advertising of effectiveness against the coronavirus
March 4, 2020	Malspam	Europe	WHO		COVID-19 themed emails coming from who.com email addresses (the real WHO has who.int addresses)
March 4, 2020	Phishing, Malware	Italy	A purported specialist offers protection advice	Trickbot	Attached word document with macros. Subject line: "coronavirus: informazioni importanti su precauzioni"

[3] https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines?utm_source=govdelivery

[4] https://www.who.int/about/communications/cyber-security

Techniques, tactics and procedures (TTPs) used in these incidents

Kill chain	Techniques and Tools	ATT&CK
Weaponisation	Can use legitimate-looking document files or images to conceal malicious code.	
Delivery	Phishing link Spearphishing Attachment Spearphishing via Service	T1192 T1193 T1194
Installation	User Execution	T1204

Recommendations and mitigations

Name	Details	ATT&CK
Restrict Web-based content		M1021
User Training		M1017
Antivirus/Antimalware		M1049
Network intrusion prevention		M1031
Execution Prevention		M1038

Traffic Light Protocol (TLP) Reference

TLP: Traffic Light Protocol	
RED	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER	Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm.
GREEN	Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels.
WHITE	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For additional details, please see https://www.first.org/tlp/