



Coronavirus – Cybercriminals Strike in Times of Fear

March 2020

Executive Summary

For cybercriminals, vulnerability and anxiety present opportunity. As the coronavirus (COVID-19) continues to spread around the world, cybercriminals are taking advantage of the widespread fear.

Over the last several weeks, we have seen an increasing wave of social engineering and phishing campaigns targeting countries in North America and Europe. For example, cybercriminals have launched websites to mimic the following healthcare authorities:


- Centers for Disease Control and Prevention (CDC) in the USA.
- Ministero della Salute in Italy.
- Health Canada.

Such look-alike websites contain malicious payloads. Visitors to these websites may unknowingly download malware on their desktop or mobile devices. To generate traffic to these websites, the cybercriminals launch targeted email phishing campaigns that manipulate people into clicking a link. The emails contain subject lines such as “Update - Coronavirus confirmed” or “Important Coronavirus Update”, playing into people’s elevated level of concern.

A sign of the growing popularity of coronavirus-themed attacks is the emergence of targeted phishing kits on the Dark Web. On several Dark Web marketplaces, hackers are offering for sale default phishing kits that bundle the interactive real-time Coronavirus map from the World Health Organization with a malicious file that functions as a pre-loader (.jar file) for additional malware modules. The following image is of one such Dark Web vendor offering a Coronavirus map phishing kit for \$200.

Coronavirus – Cybercriminals Strike in Times of Fear

FalosOfTanos
byte

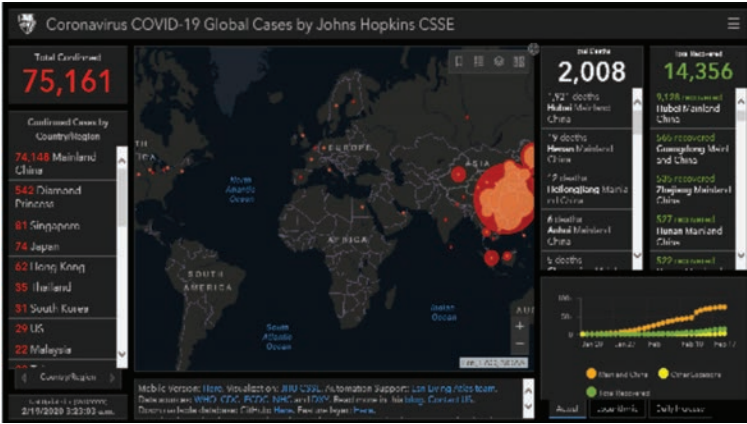


Paid registration
● 0
19 posts
Joined
02/19/20 (00 100+40)
Activity
Другое/ other

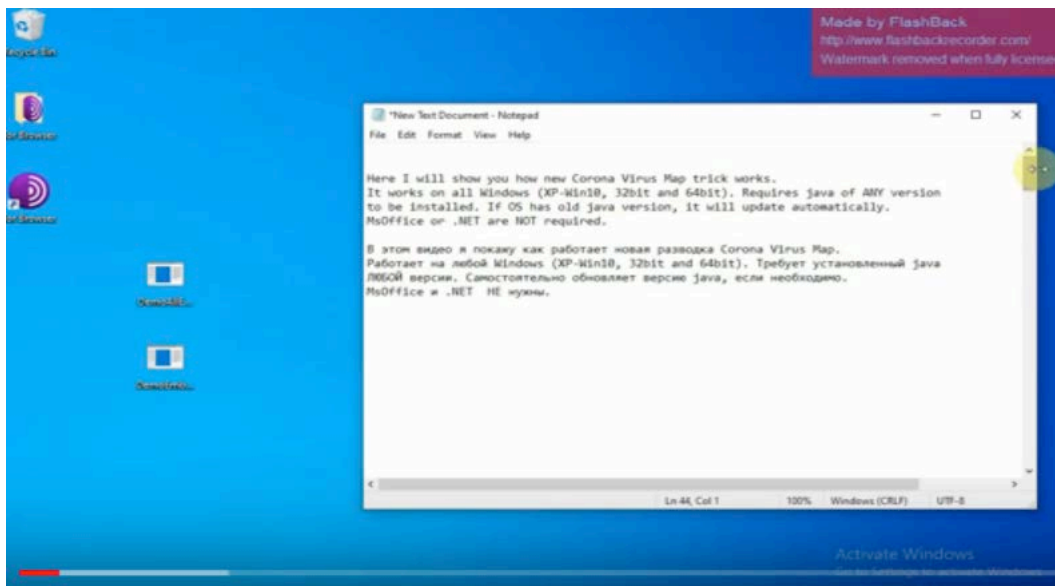
Posted February 20

New Corona Virus Map Phishing method

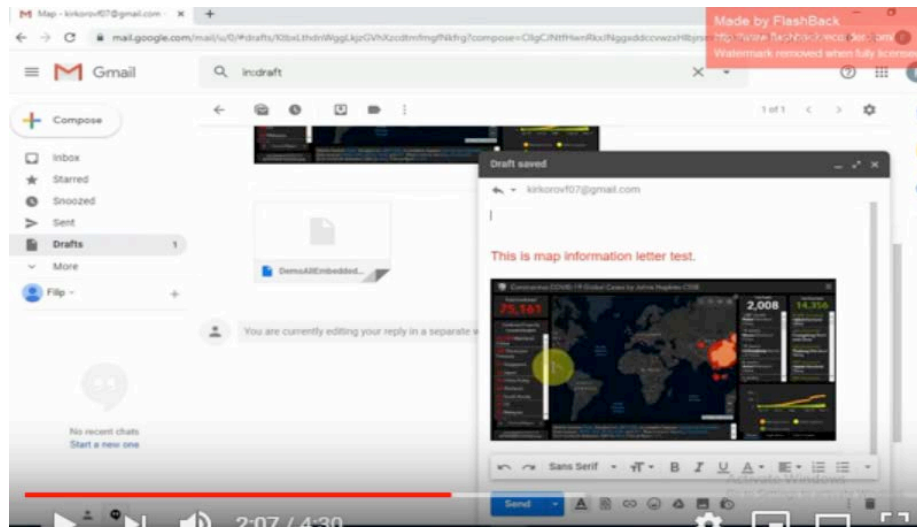
Новая разводка Карта распространения Корона Вирус



This particular cybercriminal shares a YouTube video that demonstrates the features and functionality of the phishing kit, claiming that his phishing method is able to bypass Gmail filters provided that Java is installed on the victim's device.



Coronavirus – Cybercriminals Strike in Times of Fear



Recommendations

To prevent your employees and other stakeholders from falling victims to the growing wave of Coronavirus-related cyberattacks, consider taking the following steps:

1. Educate your employees and other stakeholders about Coronavirus-related social engineering and phishing attacks.
2. Share approved websites or applications for Coronavirus-related information, and encourage the exclusive use of these resources.
3. Implement email-filtering rules to carefully review emails containing Coronavirus-related content.