
## Coronavirus Map Theme Used to Disguise and Deliver AZORult infostealer

On March 05, 2020, security researchers at Malwarebytes reported on a malicious file that leveraged the "Coronavirus map" theme to deliver AZORult infostealer. Threat actor(s) have been exploiting the fears over the Coronavirus (COVID-19) outbreak and sending out Coronavirus themed phishing emails to deliver malware such as Emotet, Remcos RAT, and Lokibot.

The program had filename "Corona-virus-Map.com" and presented itself as a piece of software claiming to show users a global heatmap of Coronavirus infection cases in real-time. The file is a console app, an executable program capable of being run by MS-DOS and Windows. Upon execution, it performs the following actions:

- Launches a web browser control that points to the legitimate Johns Hopkins Corona Virus Dashboard.
- Using the dashboard as a decoy, it installs the AZORult infostealer onto the victim machine.

AZORult then communicates with its command and control (C2) server. Based on the commands received, AZORult can perform various malicious activities including stealing credentials, cookies, histories and autofill data from various browsers, stealing data from various cryptocurrency wallets, stealing skype, telegram, steam, FTP client, email client credentials, collecting screenshots, machine information, downloading and executing files.

At the time of this writing, researchers at Malwarebytes, did not observe the malicious program to be delivered through any phishing campaign and alluded to the fact that perhaps, threat actor(s) behind the campaign are likely hosting downloads of this program on their servers and hoping for potential victim(s) to stumble upon it while looking for information on the COVID-19 infection over the internet.

For additional details please see the following online sources.

- https://thehackernews.com/2020/03/coronavirus-maps-covid-19.html
- https://tc.deloittecyber.net/auth/incident/incident.xhtml?incident=1263204#/
- https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/
- https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

DIR.TEXAS.GOV

## Assistance/Feedback/Questions?

*Office of the Chief Information Security Officer*

DIRSecurity@dir.texas.gov

**Texas Department of Information Resources**

Transforming How Texas Government Serves Texans