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/

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

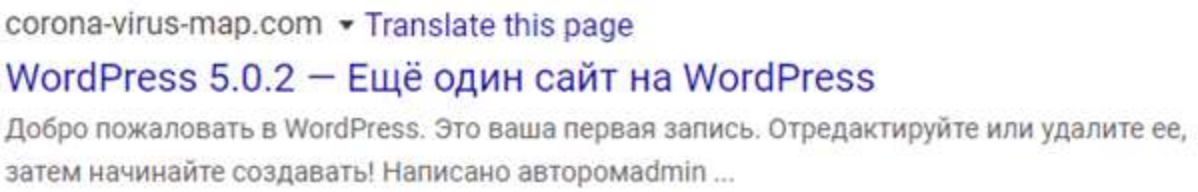

***Figure 2**. Screenshot of a Google search for the page mentioned above.*

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/.