Cybercriminals exploit coronavirus fears

James J. Giszczak, Dominic A. Paluzzi | Thursday, March 12, 2020

Cybercriminals continue to exploit any opportunity to target the data of unsuspecting victims with malicious malware, even using a growing health crisis like the coronavirus pandemic as subterfuge.

According to a report by Forbes' Zak Doffman on Wednesday, March 11, AZORult malware has found a new carrier into the systems of worried internet surfers searching for the most up-to-date news on the COVID-19 virus. Reason Labs updated a warning about the four-year-old malware now hiding behind a website offering a world map showing the spread of confirmed coronavirus cases.

David Ruiz writes on the Malwarebytes.com blog:

"Upon further analysis, we learned that this malware was actually a variant of AzorUlt, a family of spyware that steals information and sometimes downloads additional malware. We have now updated the detection name to Spyware.AzorUlt.

Unlike similar coronavirus scams we discovered last month, this threat does not rely on an email campaign."

On Tuesday, March 10, Buzzfeed's Jane Lytvynenko reported on a rash of fake emails designed to look like they are coming from Vanderbilt University and containing fake HIV results and coronavirus information:

"The emails, which include an attached spreadsheet labeled "test results," have been sent to insurance, health care, and pharmaceutical companies. When downloaded, a user is prompted to install macros,

which leads to them becoming infected with malware known as the Koadic Remote Access Trojan."

According to Lytvynenko, "Hackers are evolving their coronavirus messaging in line with the global response. Knowing that many companies asked employees to work from home, the hackers send emails that claim to be from company HR departments or executives. The victim would be asked to sign into DocuSign or Microsoft Word, which is when their credentials would be stolen."

Remember, to protect your data, only download files from trusted websites. And continue to check the credentials of any email you receive before opening attachments.

James J. Giszczak

Dominic A. Paluzzi