Microsoft finds FoxBlade malware on Ukrainian systems, removes RT from Windows app store

Home Innovation Security

Microsoft also said it will not display any Russian state-sponsored RT and Sputnik content

Written by Jonathan Greig, Staff Writer on Feb. 28, 2022

-
-
-
-
-

Microsoft says it found a new malware package -- which it calls "FoxBlade" -- hours before Russia began its invasion of Ukraine on February 24.

In a blog post, Microsoft president Brad Smith said it was coordinating its efforts to protect users in Ukraine with the Ukrainian government, the European Union, European nations, the US government, NATO, and the United Nations.

Ukraine Crisis

"Several hours before the launch of missiles or movement of tanks on February 24, Microsoft's Threat Intelligence Center (MSTIC) detected a new round of offensive and destructive cyberattacks directed against Ukraine's digital infrastructure. We immediately advised the Ukrainian government about the situation, including our identification of the use of a new malware package (which we denominated FoxBlade), and provided technical advice on steps to prevent the malware's success," Smith said.

"In recent days, we have provided threat intelligence and defensive suggestions to Ukrainian officials... This work is ongoing."

Smith noted that the cyberattacks on Ukraine seen by Microsoft have been extremely targeted and not as wide-ranging as the 2017 NotPetya attack.

But Smith said Microsoft has seen recent cyberattacks on "Ukrainian civilian digital targets, including the financial sector, agriculture sector, emergency response services, humanitarian aid efforts, and energy sector organizations and enterprises."

Microsoft has also told Ukraine's government about efforts to steal data from government sources, including healthcare information, insurance data, transportation data, and other personally identifiable information.

In addition to its efforts to help Ukraine with cybersecurity measures, Microsoft said it is also taking steps "to reduce the exposure of Russian state propaganda, as well to ensure our own platforms do not inadvertently fund these operations."

"In accordance with the EU's recent decision, the Microsoft Start platform (including MSN.com) will not display any state-sponsored RT and Sputnik content. We are removing RT news apps from our Windows app store and further de-ranking these sites' search results on Bing so that it will only return RT and Sputnik links when a user clearly intends to navigate to those pages," Smith said.

"Finally, we are banning all advertisements from RT and Sputnik across our ad network and will not place any ads from our ad network on these sites.'

"We are also focused as a company in protecting against state-sponsored disinformation campaigns, which have long been commonplace in times of war. The past few days have seen kinetic warfare accompanied with a well-orchestrated battle ongoing in the information ecosystem where the ammunition is disinformation, undermining truth and sowing seeds of discord and distrust. This requires decisive efforts across the tech sector – both individually by companies and in partnership with others – as well as with governments, academia and civil society."

Smith added that Microsoft is working with the International Committee of the Red Cross (ICRC) and multiple UN agencies on refugee support efforts.