Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats - Microsoft On the Issues

Published: 2017-12-19 · Archived: 2026-04-05 13:38:31 UTC

Dec 19, 2017

Last week Microsoft, working together with Facebook and others in the security community, took strong steps to protect our customers and the internet from ongoing attacks by an advanced persistent threat actor known to us as ZINC, also known as the Lazarus Group. We concluded that this threat actor was responsible for WannaCry, a destructive attack in May that targeted Microsoft customers. Among other steps, last week we helped disrupt the malware this group relies on, cleaned customers' infected computers, disabled accounts being used to pursue cyberattacks and strengthened Windows defenses to prevent reinfection. We took this action after consultation with several governments, but made the decision independently. We anticipate providing more information about our actions and their effect in the coming months once we have had the opportunity to analyze applicable data and information.

Today, the governments of the United States, United Kingdom, Australia, Canada, New Zealand and Japan have all announced that the government of North Korea is responsible for the activities of ZINC/Lazarus. We are pleased to see these governments making this strong statement of attribution. If the rising tide of nation-state attacks on civilians is to be stopped, governments must be prepared to call out the countries that launch them. Today's announcement represents an important step in government and private sector action to make the internet safer.

Microsoft welcomed the opportunity to work with Facebook and others in recent weeks to address this issue. As we look to 2018, it's essential that we act with shared responsibility to strengthen further the partnerships with the security community and governments to combat cyberattacks against civilians. There is much we can build on from our longstanding work with private industry partners, Interpol, Europol, the FBI and other law enforcement agencies in our ongoing efforts to combat botnets and other cybercrime.

Tags: Brad Smith, cybersecurity, malware
