Why politically motivated cyberattacks might be the new normal

June 30 2017, by Jason Kornwitz

Credit: Adam Glanzman/Northeastern University

An international cyberattack struck parts of Europe, Asia, and the United States on Tuesday, crippling tens of thousands of computers at banks, hospitals, and government offices worldwide. Initial analysis

found that the attack was designed for profit, with the hackers demanding $300 in Bitcoin in exchange for unlocking victims' screens. But further evidence now suggests that the malware was a "wiper," designed to destroy data on targets' storage systems regardless of whether they gave in to the monetary demand.

"Initial reports suggested that this was a variant of an existing strain of ransomware," said Wil Roberson, assistant professor of computer science at Northeastern, who specializes in detecting and preventing web-based attacks. "But it turns out that it was designed purely for destructive purposes."

The malware originated in Ukraine on the eve of the country's Constitution Day, leading one computer scientist to speculate that it was "aimed at generating chaos, not money." According to a *New York Times* report, many Ukrainians have cast their suspicions on Russia as the culprit.

Was this a state-sponsored attack? John Manferdelli, executive director of Northeastern's Cybersecurity and Privacy Institute, is not 100 percent sure. But he said "it certainly smells bad," referring to the high probability that Russia is the source of the virus.

Manferdelli himself is the former engineering director for production security development at Google. He noted that "cyberattacks are nothing new," explaining that hackers have been using ransomware and stealing intellectual property for years. But he added that politically motivated hacking might be on the rise, the new normal. "People forget that cyberattacks were quite common five or even 10 years ago," he explained. "What's different now is the motivation."

Robertson agreed, saying that we'll "certainly see more and more nation-state malware cropping up as cyberspace becomes more militarized as a

way to achieve geopolitical goals."

This wiper attack—like last month's WannaCry ransomware attack—reportedly used hacking tools that were stolen from the National Security Agency and leaked online by a group called the Shadow Brokers. WannaCry infected more than 300,000 computers in over 150 countries worldwide, making more than $80,000 in the process. The hackers behind the wiper, dubbed "Petya," have made less than $10,000, reinforcing the theory that money was not their primary motivation.

Robertson and Manferdelli advised ransomware victims not to pay up, even if doing so would allow them to recover their data. "Typically you don't want to pay the ransom, because there's no guarantee that you'd get your files back and you're really just sending money to a criminal enterprise," Robertson explained.

Carla Brodley, dean of the College of Computer and Information Science, noted that people could protect themselves from future ransomware attacks by updating their software and backing up their data. Running an out-of-date system, she said, is a surefire way to be hit with the next WannaCry- or Petya-like attack. "When your auto update pops up on your computer screen when you're watching Orange is the New Black," she said, "stop binge-watching the show and update your system immediately."

Provided by Northeastern University

Citation: Why politically motivated cyberattacks might be the new normal (2017, June 30) retrieved 24 May 2024 from https://phys.org/news/2017-06-politically-cyberattacks.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.