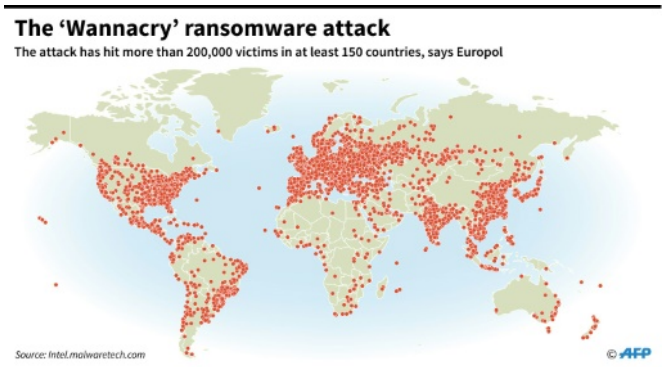
# Jury out on North Korea link to ransomware attack

25 May 2017




The "WannaCry" ransomware attack seen in a graphic on May 14, 2017

Was North Korea behind the ransomware epidemic that hit global computer networks earlier this month?

That's the subject of heated debate in cybersecurity circles after analysts found similarities in the "WannaCry" worm to other malware attributed to North Korea, including the 2014 hack of Sony Pictures and a cyberheist of millions of dollars from the Bangladesh central bank.

The security firm Symantec this week said the shared code makes it "highly likely" that the attacks were connected to the hacker group given the code name Lazarus, which many believe is North Korean.

Israel-based cybersecurity firm Intezer last week reached a similar conclusion, finding that WannaCry had "strong links to other malware families, believed to be developed by North Korean hackers, or known to be used in attacks against South Korean organizations."

Russian-based security firm Kaspersky Labs and others also pointed to a likely North Korean link.

While the evidence is not conclusive—hackers can often hide or "spoof" their real identities—North Korea is emerging as one of the likely suspects despite a strong denial by the Pyongyang envoy to the United Nations, some analysts say.

Symantec researchers said that despite the likely North Korea link, the WannaCry attacks "do not bear the hallmarks of a nation-state campaign but are more typical of a cybercrime campaign."

**Desperate for cash**

"I could easily see North Korea doing this as a way to get money," said Paul Benda, a Pentagon and Department of Homeland Security official who is now chief technology officer at Global Security and Innovative Strategies, a Washington consultancy.

"With the sanctions they are under they need cold hard cash."

Other analysts have noted that sanctions squeezing Pyongyang may be prompting desperate actions to raise cash through various channels, including cybercrime.

"While years of sanctions have isolated the Hermit Kingdom from much of the global financial system, North Korea may be seeking to fund the state's coffers through a widespread cybercrime campaign," said FireEye analyst Luke McNamara in a recent post on the Lawfare blog.

Paradoxically, he said, the effort to persuade and other nations to pressure North Korea may be encouraging further cyberattacks: "Pyongyang would be left with few options to compensate for lost income that it could ramp up as quickly as cybercrime."

The attacks discovered last week caused havoc in

global computer networks, affecting as many as 300,000 machines in 150 countries and disrupting governments and several industries. The hackers developed the virus to exploit a flaw exposed in leaked documents from the National Security Agency.

**Inconsistencies**

But despite the growing concerns over North Korea, some analysts say it's too soon to point the finger and cite inconsistencies with the Pyongyang connection.

The WannaCry attack appeared unsophisticated: researchers were able to halt the spread with a $10 purchase of a web domain that activated a "kill switch."

And various estimates showed the "ransom" raised amounted to a paltry $116,000 from 302 entities more than a week after computers were locked down.

James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, said WannaCry was "barely functional" and spread widely only because of the large number of networks and computers which failed to upgrade security and were vulnerable to the self-replicating "worm."

The hackers known as Lazarus are a sophisticated cybermercenary group, Scott told AFP. "They use elaborate traps, obfuscation techniques and wipers to eliminate digital footprints. This (WannaCry) has none of that."

More likely, Scott said, is that the attacks were carried out by hackers from China's People's Liberation Army "moonlighting" in their spare time.

Scott, who disputes the widely held belief that the Lazarus group is North Korean, said it is possible that Pyongyang has outsourced some of its cybercrime to these freelance Chinese hackers.

Analysts at Boston-based security firm Cybereason also questions the role of North Korea.

"Nothing in North Korea's past cyber campaigns or in their conventional military and foreign policy fit this mold," the researchers said in a blog.

John Arquilla, chair of defense analysis at the Naval Postgraduate School, said that despite the common patterns in the recent attacks, cyber forensics still have a long way to go to positively identify the source of an attack.

"We are not at the level of CSI," he said, referring to the popular television criminal forensics show.

"We have to be very careful about the potential for deception. I would not rush to take military or economically coercive actions on the basis of what might or might not be the truth" on the source of the attacks, Arquilla said.