Here's one tally of the losses from WannaCry cyberattack

May 25 2017, by Tim Johnson, Mcclatchy Washington Bureau

A digital worm powered by stolen National Security Agency software caused $1 billion in damages when it infected hundreds of thousands of computers in less than a week, a Florida digital security company says. And new attacks may be in the offing.

Hackers unleashed the worm, dubbed WannaCry, on May 12. Some 200,000 to 300,000 computers were affected in at least 150 countries.

"The estimated damage caused by WannaCry in just the initial four days would exceed $1 billion, looking at the massive downtime caused for large organizations worldwide," Stu Sjouwerman, chief executive at KnowBe4, a Clearwater, Fla., firm that helps firms avoid phishing efforts, wrote in a statement.

The damage estimates include loss of data, lost productivity, disruptions to business, forensic investigation, reputational harm and other factors, the company said.

The digital contagion encrypted the hard drives of computers. Hackers then demanded payment in the digital currency bitcoin to unfreeze the hard drives. The hackers provided three bitcoin wallets, or repositories, for payment of a minimum of $300.

An automated tracker of bitcoin payments reports that 302 payments have been made to the wallets, totaling $116,542, indicating that most victims paid no ransom and probably lost all the data on their computers.

Depending on one's perspective, that might seem to be a relatively small haul for the hackers, given the massive, raw pain they inflicted on users worldwide.

"I would say it's low, comparatively, especially considering the number of infections and attention it received," said Raj Samani, chief scientist at McAfee, a Santa Clara, Calif., computer software security firm.

"One theory is that it was never about the money," said Perry Carpenter, strategy officer at KnowBe4. "It was more about creating a large-scale bit of noise. The other theory is that it was about the money but it was intended to be small-scale ... and got out of hand."

Among the companies and institutions affected by the attack were FedEx, automotive plants for Renault and Nissan, Spain's telecommunications giant Telefonica, and some 48 hospitals and clinics of the British National Health Service. Russia was the nation hardest hit.

The WannaCry epidemic utilized one of a handful of powerful cybertools stolen from the NSA and leaked to the public in March by an underground group, The Shadow Brokers.

Cybersecurity experts warned this week that other leaked NSA tools have been detected and, while currently harmless, could be "weaponized" into something scarier than WannaCry.

A Croatian security adviser, Miroslav Stampar, announced Sunday on a website favored by programmers that he had discovered a new self-replicating worm, dubbed EternalRocks, that uses seven leaked NSA exploits, or techniques. EternalRocks allows hackers to dominate and remotely control infected computers, but it has yet to be detected conducting malicious activity.

The new worm could be programmed to sit silently on computers, ready to search for password files and credit card and bank account information, said John Kronick, director of cybersecurity for the advanced technology group of PCM Group.

"Very clearly, that will be more damaging because those people won't know that that's happening," Kronick said. "It'll be out the door and you won't even know it."

A debate intensified, meanwhile, about whether a hacking group linked to North Korea was behind the WannaCry epidemic.

A prominent cybersecurity firm, Symantec, said its researchers had detected multiple instances of unique code and tools used in the WannaCry epidemic that had been used previously by Lazarus, a name given to a hacking group linked to North Korea.

Symantec declared Monday that it was "highly likely" that "Lazarus was behind the spread of WannaCry." A second company, FireEye, concurred Tuesday that WannaCry shared code with attacks previously believed carried out by North Korea, including a 2014 hack of Sony Pictures and a 2016 theft of $81 million from Bangladesh's central bank.

Dissent has been vigorous, however.

"The release of attribution evidence is premature, inconclusive and distracting," James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, a Washington research center, said in a blog posting. Scott argued that Lazarus has never been proved to be a North Korean state entity and is more sophisticated than the WannaCry perpetrators.

A rogue faction of Lazarus could be involved, Scott said, although the

malware "appears to have been developed with Chinese keyboard settings and used an automatic English translation for ransom demands."

Carpenter, the KnowBe4 expert, said experts were "always looking for 'tells' within the code" and while some evidence pointed a finger at North Korea "there's no 100 percent certainty around that."

"There are other intelligence services, of course, that could insert that same bit of code as a false flag," Carpenter said. "We actually know that we (the U.S. government) do that in some cases."