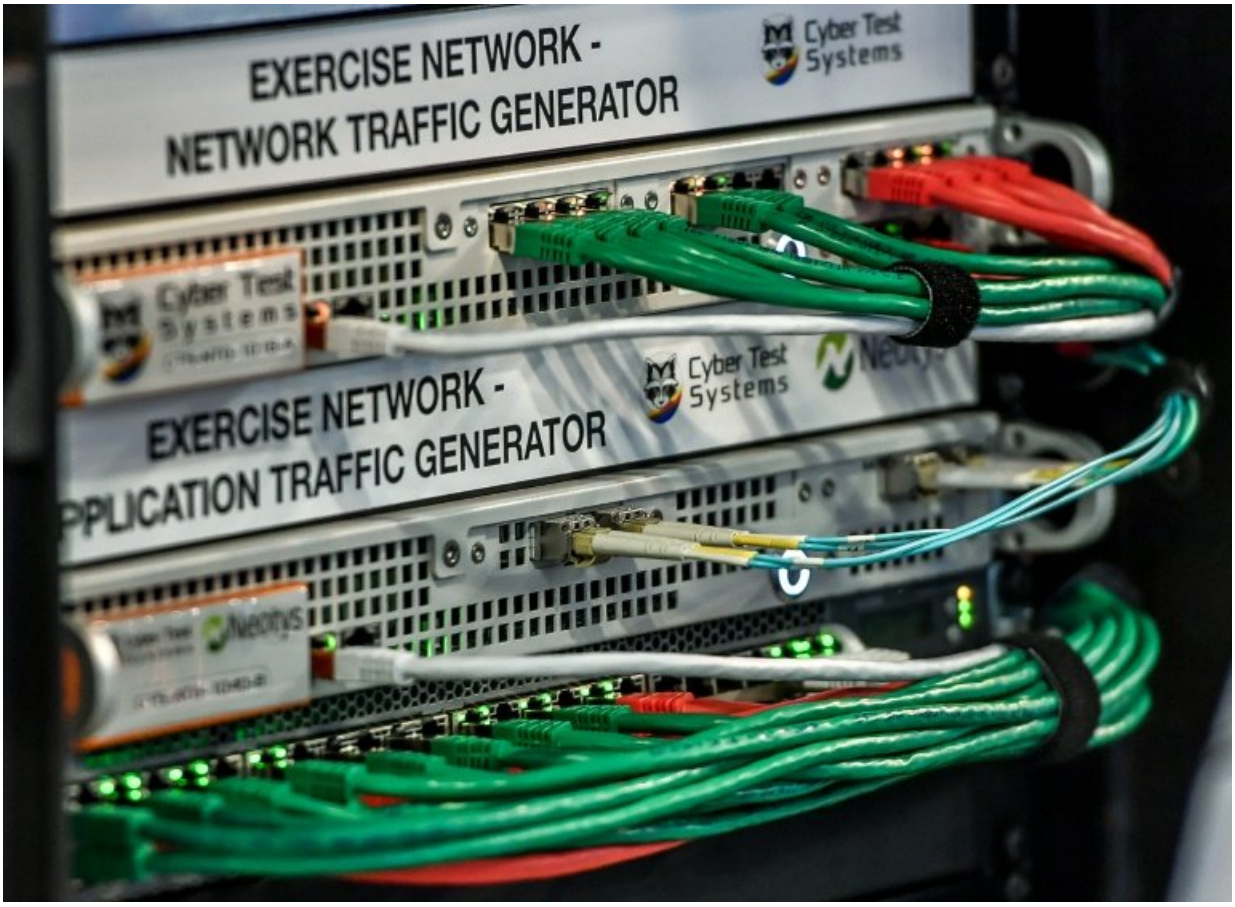
Global cybercrime costs $600 bn annually: study

February 21 2018, by Rob Lever



Cybercrime costs are rising due to increased sophisication of attackers, a new report found

The annual cost of cybercrime has hit $600 billion worldwide, fueled by

growing sophistication of hackers and proliferation of criminal marketplaces and cryptocurrencies, researchers said Wednesday.

A report by the security firm McAfee with the Center for Strategic and International Studies found theft of intellectual property represents about one-fourth of the cost of cybercrime in 2017, and that other attacks such as those involving ransomware are growing at a fast pace.

Russia, North Korea and Iran are the main sources of hackers targeting financial institutions, while China is the most active in cyber espionage, the report found.

Criminals are using cutting-edge technologies including artificial intelligence and encryption for attacks in cyberspace, with anonymity preserved by using bitcoin or other cryptocurrency, the researchers said.

"We are seeing the bad actor community taking advantage of the innovation in the technology industry," Steve Grobman, chief technology officer for McAfee, told a news conference in Washington.

Even though these technologies can offer "tremendous value" when used for legitimate purposes, they also can be adopted by criminals to hide their tracks, Grobman said.

The McAfee-CSIS report suggested cybercrime costs were rising from a 2014 estimate of $445 billion.

"We were hoping it would flatten, but we didn't see that," said CSIS vice president James Lewis.

One of the reasons for the increase, according to Lewis, is that "there's a whole 'dark web' phenomenon that creates a safe space for criminals to operate."

Cybercriminals can find a "safe" space to operate in dark web marketplaces, according to researchers

These dark web marketplaces, the report noted, allow hackers and other criminals to offer their services or sell tools which can be used for attacks, and to sell stolen credit card numbers or other valuable data.

'Russia is the leader'

Lewis said meanwhile the geopolitical risks of cybercrime are a key element in these attacks.

"Our research bore out the fact that Russia is the leader in cybercrime, reflecting the skill of its hacker community and its disdain for western

law enforcement," Lewis said.

"North Korea is second in line, as the nation uses cryptocurrency theft to help fund its regime, and we're now seeing an expanding number of cybercrime centers, including not only North Korea but also Brazil, India and Vietnam."

The report said there is often a connection between governments and the cybercrime community.

It noted that in a massive attack against US-based Yahoo, "one of the cybercriminals who hacked Yahoo at the behest of Russian intelligence services... also used the stolen data for spam and credit card fraud for personal benefit."

The study did not attempt to measure the cost of all malicious activity on the internet, but focused on the loss of proprietary business data, online fraud and financial crimes, manipulation directed toward publicly traded companies, cyber insurance and reputational damage.

The global research report comes days after the White House released a report showing cyberattacks cost the United States between $57 billion and $109 billion in 2016, while warning of a "spillover" effect for the broader economy if certain sectors are hit.

Citation: Global cybercrime costs $600 bn annually: study (2018, February 21) retrieved 9 April 2024 from https://phys.org/news/2018-02-global-cybercrime-bn-annually.html