PHYS.ORG

US cybersecurity chief warns of 'market' in malware

June 17 2009, by Andrew Beatty

More must be done to combat the lucrative trade in malicious software, which threatens sensitive government networks and personal data, the head of the US National Cybersecurity Center warned Tuesday.

More must be done to combat the lucrative trade in malicious software, which threatens sensitive government networks and personal data, the head of the US National Cybersecurity Center warned Tuesday.

In his first interview since taking up the post in March, Philip Reitinger told AFP the spread of so-called malware like botnets -- software that hijacks computers to mine sensitive data -- now constitutes an "underground market economy" that is spreading attacks.

"There is an entire community of people who are involved, organized crime is involved. Hackers now not only assemble botnets, they sell botnets. There is an underground market economy behind that.

"We have seen lately some of the risk to national government capabilities from botnet attacks," said Reitinger, who heads the Department of Homeland Security's cybersecurity operations.

His comments come just weeks after US President Barack Obama unveiled a review of cybersecurity policy, which warned the country's digital infrastructure was "not secure or resilient" to cybercrime and state-sponsored intrusions.

Reports have indicated the US electricity grid and F-35 fighter jet programs had been the target of attacks, amid dark murmurings about backing from foreign governments.

"Everyone recognizes that we are in a national security moment," said Reitinger, who joined the government after a stint as Microsoft's "Chief Trustworthy Infrastructure Strategist."

"The threats have been rising for some time and although our capabilities as a government and in fact internationally have been going up, it's I think clear that the status quo is no longer sufficient.

"Everyone thought of hackers as sort of curious kids that sat in their room and banged on the computer late into the night with their pizza boxes and, you know, they were just out there to make a name for themselves.

"Cracking is very different now, the threats have become much more sophisticated," he said.

"The hackers, who used to worry about making a name for themselves by putting graffiti on 100,000 systems, now want to attack one system and get specific information from it, or attack 50 systems and get credit card information."

Reitinger said that the trade in malware was spreading hackers' capabilities regardless of motive, and making the origin of attacks more difficult to trace.

"The same type of techniques that are used for one type of attack would be used for another type of attack. People are trying to get access to systems and get the information off them," he said.

"There is certainly a market economy for botnets, where people will buy and sell botted computers, so you could go online and say 'I'd like to launch a denial of service attack against XYZ,' and you could pay money and have that denial of service attack launched."

Reitinger said global cooperation and government measures to help businesses improve online identity checks would help improve web security.

He said he also wanted to ramp up government recruitment of cybersecurity specialists in order to boost capabilities.

Cyber attacks are thought to cost the US economy around eight billion dollars a year, although estimates including intellectual property theft put the figure at closer to one trillion dollars.

Citation: US cybersecurity chief warns of 'market' in malware (2009, June 17) retrieved 19 April 2024 from https://phys.org/news/2009-06-cybersecurity-chief-malware.html