

Cyber-warfare: Five Major Russian Banks Repel Massive DDoS Attack

By [RT News](#)

Global Research, November 10, 2016

[RT News](#) 10 November 2016

Region: [Russia and FSU](#)

Theme: [Global Economy](#)

At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries.

The attack began Tuesday afternoon, and continued for two days straight, according to a source close to Russia's Central Bank quoted by RIA Novosti. Sberbank confirmed the DDoS attack on its online services.

"The attacks are conducted from botnets, consisting of tens of thousands computers, which are located in tens of countries," Sberbank's press service told RIA.

The initial attack was rather massive and its power intensified over the course of the day.

"We registered a first attack early in the morning ... the next attack in the evening involved several waves, each of them was twice as powerful as the previous one. Bank's cybersecurity noticed and located the attack in time. There have been no problems in client online services," Sberbank representative said.

Alfabank has also confirmed the fact of the attack, but called it a "weak" one.

"There was an attack, but it was relatively weak. It did not affect Alfabank's business systems in any way," the bank told RIA Novosti.

According to Russian computer security company Kaspersky Lab, more than a half of the botnet devices were situated in the US, India, Taiwan and Israel, while the attack came from 30 countries. Each wave of attack lasted for at least one hour, while the longest one went on for 12 hours straight. The power of the attacks peaked at 660 thousands of requests per second. Some of the banks were attacked repeatedly.

"Such attacks are complex, and almost cannot be repelled by standard means used by internet providers," the news agency quoted Kaspersky Lab's statement as saying.



Octave Klabá / Oles @olesovhcom

22 Sep

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps !
pic.twitter.com/XmlwAU9JZ6



Octave Klabá / Oles
@olesovhcom

 Follow

This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

8:31 AM - 23 Sep 2016

  614  408

According to a source in Central Bank, the botnet behind the attack consists not only of computers, but also of the so-called Internet of Things (IoT) devices. Computer security experts note, that various devices ranging from CCTV cameras to microwaves, are prone to hacking and pose a significant threat when assembled into a botnet. Owners of such devices underestimate the risks and often do not even bother to change a default password. A massive botnet, able to send more than 1.5Tbps and consisting of almost 150 thousands of CCTV cameras has been reportedly uncovered in September.

According to Kaspersky Lab, it was the first massive attack on Russian banks this year. The previous attack of such a scale came in October 2015, when eight major banks were affected.

The original source of this article is [RT News](#)
Copyright © [RT News](#), [RT News](#), 2016

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [RT News](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those

who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca